Los Angeles Unified School District
Office of the Inspector General

Performance Audit of the Incident System Tracking Accountability Report

iSTAR

OA 23-1466
October 22, 2025

Sue Stengel
Inspector General

Los Angeles Unified School District
Office of the Inspector General

October 22, 2025

Ms. Maryhelen Torres, Administrator of Operations
Office of District Operations
Los Angeles Unified School District
333 S. Beaudry Avenue, 23rd Floor
Los Angeles, CA 90017

RE: Performance Audit of the Incident System Tracking Accountability Report

Dear Ms. Torres:

Attached is the final report of the Performance Audit of the Incident System Tracking Accountability Report (iSTAR). Thank you for taking the time to discuss this with us.

The objectives of our audit were to determine whether (1) user access to iSTAR was appropriate, (2) incidents were reported in iSTAR and in a timely manner, (3) incidents were updated in iSTAR, including the resolution of the incidents, (4) automatic email notifications to various departments, offices, and divisions were working as intended, and (5) schools and non-school sites were monitoring the iSTAR incidents.

Please contact our office if you have any questions.

Sincerely,

Mark H. Pearson
Digitally signed by Mark H. Pearson
DN: cn=Mark H. Pearson, o, ou, email=mark.pearson1@lausd.net, c=US
Date: 2025.10.22 12:01:50 -07'00'

Mark Pearson, CPA, CFE, CIGA
Assistant Inspector General, Audits

Eric Stengel
Digitally signed by Sue Stengel
DN: cn=Sue Stengel, o=OIG, ou=OIG, email=susan.stengel1@lausd.net, c=US
Date: 2025.10.23 10:52:40 -07'00'

Sue Stengel, Esq., CIG
Inspector General

Attachment

c: Andres E. Chait
Alfonzo C. Webb

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Los Angeles Unified School District (District) Office of the Inspector General (OIG) conducted an audit of the Incident System Tracking Accountability Report (iSTAR); the "Districtwide confidential electronic cloud-based tool to report and document incidents involving students, employees, parents, community members, and contract professionals that occur on or near District schools and sites, or in District educational programs and/or activities."[1] Types of incidents reported in iSTAR include, sex crimes, weapons possession, threats, suicide risk/ideation, bullying, fights, accidents, and arrests.[2]

The objectives of the audit were to determine whether (1) user access to iSTAR was appropriate, (2) incidents were reported in iSTAR and in a timely manner, (3) incidents were updated in iSTAR, including the resolution of the incidents, (4) automatic email notifications to various departments, offices, and divisions were working as intended, and (5) schools and non-school sites were monitoring the iSTAR incidents. The OIG performed this audit because the iSTAR application is a technology tool under the District's Strategic Plan, **Pillar 4 - Operational Effectiveness**. Pillar 4A prioritizes data-driven decision-making and the development of comprehensive data-driven systems to inform decision-making. Also, the OIG has not previously audited the iSTAR system.

Summary of Findings

- **Access assigned to iSTAR users was not always appropriate.** The OIG found that there are 7,076 iSTAR users. Of those users, 194 were granted access to view or modify all reported incidents ("system-wide (everything)" access) – access that was unnecessary to perform their job duties, beyond their job classification or assigned location, or they were users who had left the District. For example, a senior window and wall washer, who should have access to incidents related to facility maintenance, had access to view all reported incidents, including incidents involving student suicide risk and employee misconduct.

- **Not all incidents were reported in iSTAR.** The OIG identified 1,001 incidents over a six-month period, located in other District systems, that were not reported in iSTAR. These incidents included issues related to suicide risk/ideation, sex crime/sexual behavior, threats, possession of weapons, inappropriate employee conduct, illegal/controlled substances, assault and battery, injuries, school bus accidents, theft and vandalism, and disruption of school operations. Even though incidents may be reported in other systems, "iSTAR will capture more specific incident information and produce more accurate and meaningful data to find similarities in incidents so that divisions can develop solutions and strategies to address these incidents and improve the response process(es)."[3] These solutions and strategies cannot be implemented when the data is never input into the iSTAR.

- **Incidents reported in iSTAR were not always submitted in a timely manner and were not always complete.** The OIG found that 70% of iSTAR reports tested were completed correctly, 17% of the reports did not include updates, the action plan(s) taken, and the resolution of the

[1] Bulletin 5269.3 Incident System Tracking Accountability Report (iSTAR), June 20, 2022, page 1.
[2] See Appendix 2 for a full list of types of incidents that are reported in iSTAR.
[3] Bulletin 5269.2 Incident System Tracking Accountability Report (iSTAR), July 19, 2013, page 1.

incident, and 11% of the reports included updates but did not document the action plan(s) taken and the resolution of the incident.

These reports included issues related to suicide risk/ideation, sex crime/sexual behavior, threats, possession of weapons, inappropriate employee conduct, illegal/controlled substances, assault and battery, injuries, school bus accidents, accidents with injury, fighting/physical aggression, inappropriate non-sexual conduct, theft and vandalism, and disruption of school operations.

We made 14 recommendations to enhance controls and improve the District's incident reporting process. Our findings and recommendations are detailed in the Results of Audit section of this report.

INTRODUCTION

The Los Angeles Unified School District (District) is committed to supporting schools and offices to create and maintain safe and caring learning and working environments for all students and staff. The Office of District Operations (Operations) provides support and guidance toward creating and maintaining a safe environment. When incidents occur that are contrary to these goals, Operations works closely with schools and offices to coordinate responses. School principals and office administrators are responsible for reporting these incidents when they happen in District facilities or involve District students, employees, and the school community.[4] On June 20, 2022, the Division of School Culture, Climate, and Safety and Operations issued Bulletin 5269.3 (BUL-5269.3)[5] detailing procedures and guidelines for reporting incidents.

"Accurate reporting enables the Local Districts (LD) [Regions], Central Offices, and other responders to allocate appropriate resources to address incidents and provide support to schools, offices, and those affected."[6]

Table 1 below summarizes the iSTAR reports and issue types reported during the fiscal years 2021-2022 and 2022-2023. The number of issue types exceeded the number of incidents, as some reports contained multiple issues. The number of iSTAR reports increased in the fiscal year 2022-2023 compared to the fiscal year 2021-2022, but the percentage of issue types between school and non-school/office sites remained constant.

[4] Bulletin 5269.3 Incident System Tracking Accountability Report (iSTAR), June 20, 2022,pages 6 and 7.
[5] Ibid.
[6] Ibid, page 1.

Table 1
iSTAR Reports and Incident Types
Fiscal Years 2021-2022 and 2022-2023

	Fiscal Year 2021-2022			Fiscal Year 2022-2023		
Location Type	**No. of iSTAR Reports**	**No. of Issue Types**	**Percentage of Issue Types**	**No. of iSTAR Reports**	**No. of Issue Types**	**Percentage of Issue Types**
Schools	36,541	42,290	97%	49,059	56,754	97%
Non-schools/Offices	1,323	1,427	3%	1,369	1,490	3%
Grand Total	**37,864**	**43,717**		**50,428**	**58,244**	

Source: 2021-2022 iSTAR Annual Report[7] and 2022-2023 iSTAR Annual Report.[8]

Table 2 summarizes the top five issue types reported during fiscal years 2021-2022 and 2022-2023.

Table 2
Top Five Issue Types
Fiscal Year 2021-2022 and 2022-2023

Fiscal Year 2021-2022		Fiscal Year 2022-2023	
Issue Type	**Percentage of Issue Type**	**Issue Type**	**Percentage of Issue Type**
Suicide Ideation/Behavior	19%	Suicide Risk	23%
Other[9]	8%	Accident	10%
Accident With Injuries	8%	Fighting/Physical Aggression	10%
Self-injury/Cutting	5%	Medical	8%
Threatened/Caused/Attempted Physical Injury	4%	Inappropriate Conduct	7%

Source: 2021-2022 iSTAR Annual Report[10] and 2022-2023 iSTAR Annual Report.[11]

See Appendix 2 for a list of all current issue types in iSTAR and their definitions.

iSTAR is accessed through the District's single sign-on (SSO) account.[12] School administrators have automatic access to iSTAR. They can complete, submit, and view all reports associated with their school and can grant or modify access for additional school staff.[13] Administrators or

[7] iSTAR Annual Report 2021-2022.
[8] iSTAR Annual Report 2022-2023.
[9] The "Other" issue type was related to incidents reported as utility failure, medical, medication error, environmental hazard, odor, vandalism or property damage, trauma, inappropriate sexual behavior, bullying, hate crime, discrimination or harassment, sexual harassment and law enforcement activity.
[10] iSTAR Annual Report 2021-2022.
[11] iSTAR Annual Report 2022-2023.
[12] The District assigns employees and non-employees an SSO account. The SSO account is an identification method that enables users to log into the District's email and applications, streamlining the authentication process for users. iSTAR can only be accessed with an active SSO account. An SSO account is disabled when an employee or non-employee retires or separates from the District.
[13] School administrators grant, modify, or remove access for additional staff through Operations' Principal's Portal. The Principal's Portal is an online tool/site developed to help school administrators access a variety of District systems in a single place to certify required activities and complete mandated reports.

supervisors at central offices or non-school sites can request access for themselves and appropriate staff by submitting a completed iSTAR Access Request Form[14] to Operations. Each user is assigned three security privilege levels in iSTAR, including an access type, one or more access sites, and a user role.

Table 3 below describes the three levels of security.

Table 3
iSTAR Security Levels

Security Level	Description
Access Type	Access types include: ▪ "system-wide (everything):" access to all incidents reported by all users or sites. ▪ "scope access (roll-up):" access to one or a limited number of sites and can only access incidents reported by those sites. ▪ "self-reported:" the user can only *create* incident reports for their assigned site(s) but cannot *submit* incident reports. Submission is generally done by an administrator.
Access Site	Users can be granted access to one or more sites (i.e., school, region, division, and central office or department).
User Role	There are 20 user roles available in iSTAR. Each role has specific entitlements that can be a combination of multiple rights. These rights include creating, modifying, submitting, approving, and deleting incidents and receiving or suppressing automatic email notifications from iSTAR. These notifications are generated when incidents or updates are submitted. According to Section I of BUL-5269.3, user roles created for school staff include "Designee 1," "Designee 2," and "Designee N." ▪ Designee 1 access is generally granted to administrators and school administrative assistants, who have the same access rights as a principal. ▪ Designee 2 is generally granted to plant managers, cafeteria managers, deans, counselors, psychiatric social workers (PSW), and pupil services and attendance counselors (PSA) who can create and request approval (also known as soft-submit) of created incidents and cannot access and update incidents they did not create. ▪ Designee N access is granted to school nurses and has the same access rights as Designee 2 but can access and update incidents created by others with issue types related to accidents, head injury, medical, suicide risk, and threats. ▪ The Principal or Designee 1 must approve or submit all incidents created by Designee 2 and Designee N.

At the time of this audit, there were 7,076 iSTAR users. 485 had "system-wide (everything)" access or "scope access" that allowed them access to every site (6.85%),[15] and 6,591 (93.1%) had other types of limited access (limited access).

[14] iSTAR Access Request Form.
[15] The 485 users were comprised of 453 users with the "system-wide (everything)" access type and 32 users who did not have the "system-wide (everything)" access type but had the "system-wide" site access.

RESULTS OF AUDIT

The objectives of the audit were to determine whether (1) user access to iSTAR was appropriate, (2) incidents were reported in iSTAR and in a timely manner, (3) incidents were updated in iSTAR, including the resolution of the incidents, (4) the automatic email notifications to various departments, offices, and divisions were working as intended, and (5) schools and non-school sites were monitoring iSTAR incidents.

Finding No. 1 – Access assigned to iSTAR users was not always appropriate.

Criteria

The District's Bulletin-114700 (BUL-114700), Access to Critical Information Systems "defines general guidelines for managing access to information systems that support critical District operations."[16] Section II of Bulletin-114700 states that "privileges must be assigned based on roles or job code and are allocated automatically once an employee is hired or manually by the system owner. Individual users must be assigned to an already-defined role and cannot be granted additional, unique privileges outside their assigned role. For example, a teacher would not be assigned additional privileges that other teachers do not have to perform their assigned duties."[17] BUL-114700 defines the guidelines for managing access to information systems that support critical District operations.

Condition

There were 7,076 active iSTAR users as of December 20, 2022. To determine whether the user access to iSTAR was appropriate, the audit team separated the total number of users into two sets of groups; one with full access to view or modify incidents by all locations, and the second one, those with limited access.

The OIG determined that 485 of those users had access to view or modify incidents reported by all locations. The OIG selected 214 users to test whether those users had more access privileges than what we assessed they needed based on their job responsibilities and the locations where they worked. We found that 194 of 214 (84%) of the users had inappropriate access that was not needed to perform their duties; these users had access to sensitive and private data/information from locations throughout the District. Table 4 details the results of our testing:

[16] Bulletin 114700.
[17] Bulletin 114700 Access to Critical Information Systems, October 11, 2021.

Table 4
Results of Testing
Users With Access to View or Modify All Reported Incidents
As Of December 20, 2022

No. of Users	Percentage of Users Tested	Description of Finding
20	9%	Users had job responsibilities that needed access to view or modify incidents reported by all locations.
180	84%	Users had access to view or modify incidents reported by all locations, allowing these users to access sensitive and/or confidential information, inconsistent with District policy. For example, a senior window and wall washer, who should have access to incidents related to facility maintenance, had access to view all reported incidents, including incidents involving student suicide risk and employee misconduct.
14	7%	Users that should have been deactivated because they left the District.

From the 6,618 iSTAR users with limited access, the OIG tested a statistically random sample[18] of 138 active users to determine if each user was granted the least privileged access[19] and user role[20] to perform their job duties. We found that 30 (or 22%) users were granted inappropriate access that was not needed to perform their duties.[21] Table 5 details the results of our testing:

Table 5
Results of Testing
Statistical Random Sample of Users With Access to iSTAR
As Of December 20, 2022

No. of Users	Percentage of Users	Description of Finding
108	78%	Users had appropriate access or the least privileged access and user roles to perform their job duties and retained appropriate access.
13	9%	Users had additional privileges or incorrect user roles not needed for their job duties. For example, a school nurse was granted the user role of "Designee 1" with the same access privileges as the school principal. According to District policy, school nurses should be assigned the "Designee N" user role, which can create and update incident reports but, unlike a principal, cannot approve or submit incidents.
13	9%	Users that should have been deactivated because they left the District.
4	3%	Users had access to incidents reported by locations they were not assigned to during the audit.

[18] Statistical sampling is a selection method that is representative of a population. A statistical sample is used to assess the characteristics of a whole population.
[19] The least privileged access is a security concept in which a user is given the minimum level of access or permission needed to perform this job.
[20] There are 20 user roles available in iSTAR. Each user role has specific entitlements that include one or more rights, which include the right to create, modify, submit, approve, and delete incidents, and the right to receive or suppress the automatic iSTAR email notifications.
[21] Job duties were based on the employee's assigned job classification in the District's Systems, Applications, and Products (SAP). SAP is a software application utilized for the management of various business processes that include payroll, accounting, human resources, and the procurement of goods and services.

In total, the OIG tested the access of 352 of 7,076 (5%) iSTAR users, focusing on those users with view and modify access to all sites.[22] We found that more than 60% of the access to all site incidents was inappropriate.

Refer to Appendix 1 for a detailed audit methodology.

Effect

The conditions described above allowed for inappropriate access and potential use of confidential and protected personal information, unauthorized changes, or deletion of reported incidents, subjecting the District to potential liabilities.

Cause

Based on interviews conducted with 60 school principals, the personnel in the Regional Offices, and the Administrator of Operations (AO), and the iSTAR System Administrator, the conditions described above occurred because:

1. There was no formal periodic review (at least once per year) of all iSTAR users and their access privileges for appropriateness.[23] According to Operations, a new iSTAR application was implemented during the fiscal year 2020-2021. School and office administrators were asked to perform a one-time review of access privileges for all their respective iSTAR users during the implementation of the new iSTAR application during the fiscal year 2020-2021.
2. A single person performed the user access permission process without a secondary review. iSTAR and the Principal's Portal allowed the system administrator and school principals to grant access to central office personnel and school staff, respectively.
3. Some school administrators stated they were unaware that granting, modifying, and removing staff access privileges was performed through the Principal's Portal. However, Operations stated that job aids were available in the Principal's Portal to guide the principals.
4. Some school administrators also stated they were unaware of the need to remove access for staff who left the school.

Recommendations

District Operations should:

Recommendation No. 1: Work with Information Technology Services (ITS), schools, and offices to complete a comprehensive review of all iSTAR users' privileges to ensure their access rights and user roles are aligned with their job duties.

[22] The 214 was a sample of the 485 users mentioned above.
[23] BUL-114700 requires system owners to conduct "reviews of access rights granted to general users annually and twice a year for privileged users." Privileged users are those with elevated access to systems and security functions.

District Operations' Response to Recommendation No. 1: Operations agreed with the recommendation and has continued to work with ITS to complete a comprehensive review of all iSTAR users' privileges annually to align with their job duties.

Implementation Date: Implemented

Recommendation No. 2: Work with ITS to implement periodic reviews of all iSTAR users and their access privileges (at least annually) for general users and semi-annually for privileged users.

Operations stated that they had performed reviews of user access following our audit and identified approximately 1,800 users that should be deactivated. OIG obtained access to iSTAR and independently validated that 1,762 user accounts were deactivated.

District Operations' Response to Recommendation No. 2: Operations agreed with the recommendation and has implemented a system in place with ITS to periodically review an iSTAR user list annually.

Implementation Date: Implemented

Recommendation No. 3: Revise the access permission process to include a secondary review from a different administrator, Operations Coordinator (OC), or higher-level authority.

District Operations' Response to Recommendation No. 3: Operations disagreed with our recommendation and stated that it has always implemented a secondary review of user access requests from Division leadership, Region-Administrators of Operations, and District Operations leadership.

OIG's Response: The OIG acknowledges that user access requests are reviewed by the Division and/or Administrator of Operations, as well as District Operations leadership. However, the OIG recommends implementing a secondary review of the user access configuration in iSTAR after approval by District Operations leadership. This additional step will help ensure that users are accurately set up in iSTAR and granted privileges consistent with the approved access request.

Recommendation No. 4: Work with ITS to complete a review of the iSTAR security configuration, the access types, access sites, and user roles to ensure the least privileged access is granted to users. If necessary, reconfigure or add an additional level of security, delete, revise, or create new access types, sites, and user roles.

District Operations' Response to Recommendation No. 4: Operations agreed with our recommendation and has collaborated with ITS to review access requests and roles.

Implementation Date: Implemented

Recommendation No. 5: Create a training program (in-person or virtual) for administrators about access permission, the existence of job aids, the importance of role-based access controls, and the risks of granting excessive access privileges.

District Operations' Response to Recommendation No. 5: Operations disagreed with our recommendation and stated that it has been providing virtual training annually and will continue to be offered to all users on access permission, the existence of job aids, the importance of role-based access controls, and the risk of granting excessive access privileges.

OIG's Response: The OIG acknowledges the annual virtual Operations training. However, an enhanced and focused program for administrators would reduce the risk of excessive access, strengthen security, and ensure policy compliance.

Recommendation No. 6: Program iSTAR to automatically align access type, site access, and user role assignments with Human Resources data, ensuring access privileges are updated for employees no longer assigned to the site and reducing the possibility of human error and oversight.

District Operations' Response to Recommendation No. 6: Operations disagreed with our recommendation and believes the current approval layers are sufficient to evaluate and assign access based on employee roles. However, Operations is working with ITS to explore the feasibility of using the District's oneAccess system for iSTAR access requests.

OIG's Response: The OIG supports Operations' plan to explore the feasibility and migrate the access request process to oneAccess, the system used by ITS to manage user accounts for other critical District applications.

Finding No. 2 – Not all incidents were reported in iSTAR or in a timely manner.

64% of the reportable incidents identified by the OIG were not reported in iSTAR.

Criteria

Section V of BUL 5269.3 states that "incidents of a critical or serious nature that impact the school operations must be completed and electronically submitted as soon as possible the same day that the incident occurred. Less serious incidents should be completed and electronically submitted within 24 hours."[24]

Condition No. 1 – Incidents were not reported in iSTAR

We obtained data captured in various District applications other than iSTAR to identify incidents that should have been reported in iSTAR from July 1, 2022 to December 31, 2022. Appendix 4 summarizes the name of the division or department, and the name and description of their respective system application(s).

From the various system applications, we identified 1,564 incidents[25] that should have been reported in iSTAR. Of those 1,564 incidents, we found 563 iSTAR reports that matched those incidents.

[24] Bulletin 5269.3 Incident System Tracking Accountability Report (iSTAR), June 20, 2022.

[25] The 1,564 incidents we identified were based on all incidents provided by the TSD and SR, and all incidents provided by DNS, SMH, LASPD and M&O for a statistical random sample of 119 schools. Approximately 199,000 incidents and cases were provided by the various offices.

However, the OIG did not find an iSTAR report for the remaining 1,001 incidents. Unreported incidents included issues related to suicide risk/ideation, sex crime/sexual behavior, threats, possession of weapons, inappropriate employee conduct, illegal/controlled substances, assault and battery, injuries, school bus accidents, theft and vandalism, and disruption of school operations.

According to Operations, training efforts have emphasized the importance of reporting incidents in iSTAR. This focus has led to an increase in the number of reports filed in iSTAR, although it does not necessarily indicate a rise in actual incidents following our audit.

Condition No. 2 – Incidents were not reported timely

We reviewed the information entered in iSTAR for a statistically random sample of 116 iSTAR reports from July 1, 2021 to December 31, 2022 to determine whether the incidents were submitted within 24 hours of the incident date. Table 6 summarizes the results of our testing.

Table 6
Results of Testing
Statistical Random Sample of iSTAR Reports
July 1, 2021 to December 31, 2022

No. of iSTAR Reports	Percentage of iSTAR Reports Tested	Description of Finding
76	65%	The iSTAR report was submitted on time.
31	27%	The iSTAR report was not submitted on time.
7	6%	The incident date was not included in the iSTAR report.
2	2%	The iSTAR report was created but not submitted. A notification for new incidents is not sent unless submitted.

Incidents that were not reported on time and reports with missing dates included issues related to suicide risk/ideation, threats, accidents resulting in injuries, injuries, fighting/physical aggression, inappropriate non-sexual conduct, and disruption of school-wide activities.

Effect

The two conditions described above could lead to unresolved and/or untimely resolution of incidents and issues, resulting in potentially unsafe learning and work environments for students and staff, reduced academic achievement, a reduction in staff productivity, and inaccurate or unidentified statistics and trends.

Cause

Based on our interviews conducted with 60 school principals, the Region AOs, Transportation Services Division staff, Operations AOs, and Operations Coordinators (OC), the conditions described above occurred because:

1. Not all administrators received training, understood which incidents required an iSTAR report, or the training provided to administrators did not include specific examples of incidents and issue types. According to some administrators, training related to iSTAR is usually brief and included as part of the principals' meeting after school hours. Some administrators stated that it is sometimes challenging to match the incident to one or more issue types in iSTAR.
2. Some administrators do not report incidents they consider to be insignificant. For example, one administrator stated that vandalism and graffiti that the plant manager can fix are not reported in iSTAR. Another administrator stated that incidents occurring outside of the school perimeter are not reported.
3. Administrators are not constantly monitoring iSTAR to ensure all incidents are reported.
4. Operations does not have full-time staff solely responsible for monitoring iSTAR and assisting schools and offices with iSTAR-related issues to ensure incidents are reported and reported in a timely manner.
5. Some administrators stated that they do not have sufficient resources and are constrained by other priorities (such as instructional duties, resolving incidents, and ensuring the safety of staff and students) over entering any reports in iSTAR. According to the administrators, most reports are filed after school hours at night or whenever time permits.
6. According to Region AOs, six to seven Region OCs are in each of the four District regions. However, the average number of schools and students assigned per OC is different because each region has a different number of schools and enrolled students. One Region AO stated that the OCs in his region were assigned to: (1) more schools, (2) managed more schools ranked with the highest/high school's Student Equity Needs Index (SENI),[26] and (3) have more students compared to other OCs in other regions. See Appendix 3 for a comparison of this information.
7. Administrators and staff lose efficiencies when manually entering incidents into iSTAR and other District applications, such as My Integrated Student Information System (MiSiS),[27] Welligent.net, Welligent.com, MAXIMO, RMS, CAD, and BusOps.

Recommendations

District Operations should:

Recommendation No. 7: Work with the administrators and Region AOs to reinforce District policy that all required incidents are submitted, and issue types are reported in iSTAR.

District Operations' Response to Recommendation No. 7: Operations agreed with our recommendation and has implemented monthly training reminders and reports for Region AOs and

[26]The SENI is a weighted formula based on various academic indicators such as primary literacy test and A-G completion rate, school climate indicators such as suspension rates and absenteeism, and school demographics. The District implemented the SENI to allocate funds to targeted student groups, such as low-income, English Learners and foster care students, to close the equity gap.
[27]MiSiS is a modernized all-in-one student information solution that captures and allows users to view student information such as student discipline and academic progress.

OCs, along with iSTAR system reminders shared with school leaders. Additionally, Operations is working to develop automated monthly notifications.

Implementation Date: November 2025

Recommendation No. 8: Work with the Human Resources Division to implement a virtual training program detailing the iSTAR reporting requirements, the required incidents, and issue types. The virtual training should be required to be completed by all District staff annually.

District Operations' Response to Recommendation No. 8: Operations disagreed with our recommendation and stated that it provided ongoing virtual training annually and will continue to be offered to all users.

OIG's Response: The OIG acknowledges the annual virtual Operations training. However, a more focused, mandatory program for all District staff would improve reporting accuracy, reduce errors, and strengthen policy compliance. According to Operations, post-audit Operations training has emphasized the importance of reporting incidents in iSTAR. This has resulted in an increase in reports filed, though not necessarily a rise in actual incidents.

Recommendation No. 9: Develop detailed guidance or job aids for submitting incidents and the issue type(s) that must be reported in iSTAR, required updates, examples of action plans, and proper resolution of incidents. A link to the guidance or job aids should be included in iSTAR for accessibility.

District Operations' Response to Recommendation No. 9: Operations disagreed with our recommendation and stated that it has provided job aids for submitting incidents and updating issue type(s). However, additional job aids will be part of the updated iSTAR bulletin to provide more guidance.

OIG's Response: The OIG supports Operations' plan to develop additional job aids. Clearer guidance on selecting incident types, required updates, and examples of reportable incidents and action plans would improve reporting accuracy, reduce errors, and enhance policy compliance.

Recommendation No. 10: Require administrators and AOs to monitor iSTAR and certify periodically that all required incidents were submitted, submitted timely, included all applicable issue types, were updated regarding progress, action plan(s), and resolution, and closed when resolved.

District Operations' Response to Recommendation No. 10: Operations agreed with our recommendation. Administrators and AOOs currently monitor iSTAR and reports, and work closely with site administrators. Error reports are sent to Region Operations to follow up with schools, and automated notifications will be sent to the school principals of pending iSTAR reports that need to be closed.

Implementation Date: November 2025

Recommendation No. 11: Develop metrics to monitor incidents and resources to ensure incidents are addressed effectively and in a timely manner.

District Operations' Response to Recommendation No. 11: Operations agreed with our recommendation. Administrators and AOOs currently monitor iSTAR and reports, and work closely with site administrators. Error reports are sent to Region Operations to follow up with schools, and automated notifications will be sent to the school principals of pending iSTAR reports that need to be closed.

Implementation Date: November 2025

Recommendation No. 12: Work with the system owners of other District applications to develop system interfaces that automatically populate incidents in iSTAR, increasing efficiency and reducing potential human error and omissions.

District Operations' Response to Recommendation No. 12: Operations disagreed with the recommendation and stated that developing interfaces is not feasible due to iSTAR's unique platform. Additionally, iSTAR was built as a confidential platform protected by the Attorney-Client Privilege.

Finding No. 3: Some incidents reported in iSTAR were incomplete. Of a statistically random sample of 116 iSTAR reports[28] tested by OIG, 70% were completed correctly. 17% of the reports did not include updates, the action plan(s) taken, and the resolution of the incident, and 11% of the reports included updates but did not document the action plan(s) taken and the resolution of the incident.

Criteria

Section II of BUL 5269.3 states that updates should be provided in a timely manner, and certain issue types require additional forms to be filled out with more detailed information about the incident.[29] These forms include the Risk Assessment Referral Data (RARD), Medication/Protocol Error Form, Head Injury Form, and Injury/Illness Form.[30]

Refer to Appendix 2 for a current list of issue types that are required to be reported in iSTAR.

Condition No. 1 - Some incidents reported in iSTAR were incomplete.

The OIG reviewed detailed information in iSTAR for the sample of 116 created or submitted iSTAR reports to determine whether updates were entered into iSTAR, action plans were taken and documented, and the resolution of the incidents was entered in iSTAR. Table 7 below summarizes the results of our testing.

[28]The 116 iSTAR reports was a statistically random sample of all incidents (8,819) incidents reported by 119 schools.
[29]The additional information included witnesses, cause of the incident, factors that contributed to the incident, violation of district policies, training, actions taken to prevent reoccurrence of the incidents, whether the parent or guardian was notified, whether the person went to a hospital or clinic, whether the person returned to school or work site, the level of risk (for incident requiring a RARD), etc.
[30]Bulletin 5269.3 Incident System Tracking Accountability Report (iSTAR), June 20, 2022, page 5.

Table 7
Results of Testing
Statistical Random Sample of Submitted iSTAR Reports
July 1, 2021 to December 31, 2022

No. of Submitted iSTAR Reports	Percentage of iSTAR Reports Tested	Description of Finding
81	70%	The submitted iSTAR report included updates, the action plan(s) taken, and the resolution of the incident.
20	17%	The submitted iSTAR report did not include updates, the action plan(s) taken, and the resolution of the incident.
13	11%	The submitted iSTAR report included updates but did not document the action plans(s) taken and the resolution of the incident.
2	2%	The incident was created in iSTAR but not submitted for review.
116	100%	

iSTAR reports without updates, action plans, and/or incident resolutions included issues related to suicide risk/ideation, threats, sex crime/sexual behavior, sexual harassment, accidents resulting in injuries, injuries, fighting/physical aggression, inappropriate non-sexual conduct, disruption of school-wide activities, child annoyance and utility failure.

Our testing also found that the required forms were not completed or were incomplete for 37 incidents. These forms included the Illness/Injury Form, Head Injury Report, and the Risk Assessment Referral Data.

Condition No. 2 - Not all issue types were reported for each incident.

We reviewed the same sample of 116 iSTAR reports to determine whether all issue types were reported for each incident. iSTAR allows users to report multiple issue types that best describe the incident.

The OIG identified 14 incident reports (12%) that did not include all applicable issue types. For example, a student injury sustained from a fight with another student was reported as a "Head Injury" and not both "Head Injury" and "Fighting/Physical Aggression." A school lockdown was reported as "Disrupted School-Wide Activities" instead of both "Disrupted School-Wide Activities" and "Lockdown."

Other Observation

During our testing, we noted that the status of 95 or 83% of the 114 (this does not include the two reports that were created but not submitted) submitted iSTAR reports remained "open." However, we determined that the status for 86 of the 95 (90.5%) reports should have been "closed" based on the information entered in iSTAR. We could not determine the status of the remaining nine incidents due to insufficient information entered in iSTAR.

Effect

As a result, the District's exposure to potential legal liabilities may be increased if the District is not able to demonstrate (document) that employees have taken appropriate action(s) to address incidents and resolve the issue(s) in a timely manner.

Cause

Based on our interviews of 60 school principals, the Region AOs, the Transportation Services Division, and Operations, these conditions occurred because:

1. Not all administrators received training, understood the reporting requirements, or knew when to consider an incident closed. Administrators stated that some incidents took longer to close if multiple follow-ups were needed, as was the case with students at risk of suicide.
2. Administrators were not always monitoring iSTAR to ensure that updates were provided, and action plans and resolutions were documented.
3. Operations did not have full-time staff solely responsible for assisting schools and offices with iSTAR-related issues and monitoring iSTAR to ensure that: (i) updates on prior incidents were provided, (ii) action plans and resolutions were documented, and (iii) incidents were closed when resolved.
4. Some administrators stated that they do not have sufficient resources and are constrained by other priorities such as instructional duties, resolving incidents, and ensuring the safety of staff and students before entering updates, action plans, and resolutions in iSTAR.

Recommendations

District Operations should:

Recommendation No. 13: Work with the administrators and Region AOs to provide updates for reported incidents, ensure action plan(s) and resolution(s) are documented, and close reports for incidents that have been resolved. Configure the iSTAR system to include automatic notifications when incidents have been open for more than a certain number of days, or when the incident information is incomplete.

District Operations' Response to Recommendation No. 13: Operations agreed with our recommendation and is working with Region Operations and AOOs to review error reports, which are shared with schools alongside monthly professional development guidance during Operations meetings. Region Operations follows up with schools, and automated notifications are being developed to alert principals of pending iSTAR reports requiring closure.

Implementation Date: November 2025

Recommendation No. 14: Include required updates, documentation of action plans and resolutions, and examples of incidents considered closed as part of the training program.

District Operations' Response to Recommendation No. 14: Operations agreed with our recommendation and will continue providing training on creating and resolving incidents. Discussions regarding legal documentation will be held with the Office of the General Counsel.

Implementation Date: Implemented

See Recommendation Nos. 7 to 10 under Finding No. 2.

Finding No. 4 - The automated email notifications via iSTAR to various departments, offices, and divisions were working as intended.

Criteria

Section VIII of BUL 5269.3 states that "notifications of all school-site incidents reported in iSTAR are automatically sent to the appropriate Local District, Central Offices, the Office of District Operations, the respective Board Member or representative, the Administrator of Operations, and the Operations Coordinator(s)."[31] According to the Operations OC, iSTAR is programmed with an automated email notification capability for submitted reports. Certain offices and the Region AOs and OCs are automatically set up to receive email notifications from iSTAR for all submitted reports. Employees with certain user roles also have the option to suppress email notifications through their user profile, even if they are set up to receive automated iSTAR notifications.

Condition

We performed a walkthrough of the iSTAR automated email notifications with the Operations AO and an OC, reviewed the automated email notification setup in iSTAR for a Region's AO, requested to be set up to receive the automated email notifications from iSTAR, and confirmed that the email notification via iSTAR was working as intended. We received 45 automated email notifications for all 45 newly submitted incidents during a four-hour period we tested from 9:00 a.m. to 1:00 p.m. on September 6, 2023.

We also confirmed with the Region's AO during our visit and interview with them that they are receiving automated email notifications from iSTAR for submitted incident reports, including submitted updates on previously reported incidents. According to the Region AOs, the Region OCs were also involved in the incidents and provided school guidance and support.

Schools and non-school sites monitored the iSTAR data to address incidents. School principals or office administrators reviewed submitted incidents.

Criteria

BUL 5269.3 states that iSTAR captures specific incident information and produces accurate and meaningful data. Accurate reporting enables offices and other responders to develop solutions and

[31] Bulletin 5269.3 Incident System Tracking Accountability Report (iSTAR), June 20, 2022, page 8.

strategies and allocate appropriate resources to address incidents and improve the response process(es).[32, 33]

Section V of BUL 5269.3 states, "principals and office administrators should review all reports submitted by their designee(s) or by the LASPD for accuracy, completeness of information, and follow-up, as necessary." Section VI also states that AOs should review iSTAR reports to determine whether any additional resources or assistance might be needed to address incidents.[34]

Condition

We visited and interviewed a sample of 60 school principals,[35] the Region AOs, and the Director of the Transportation Services Division to determine whether they were monitoring iSTAR data and addressing incidents. Based on our visits and interviews, the following was revealed:

- The school principals stated that they work with their designee(s), if any, and the assigned Region OC to address issues.
- The Region AOs confirmed that they have assigned an OC to each school to provide support and are involved in all incidents. Each OC receives notifications of submitted iSTAR reports and periodically reviews the status of reported incidents.
- Three of the four Region AOs also stated that Operations assists them in generating reports to identify trends.
- Operations publishes an iSTAR annual report summarizing the number of reports and top issue types for the fiscal year by Local District/Region, Board District, and location type (e.g., elementary school, middle school, high school, and non-school locations). Operations provided the audit team with two iSTAR annual reports for the fiscal years 2021-2022[36] and 2022-2023.[37]

We also reviewed the activity history[38] in iSTAR for the statistically random sample of 116 iSTAR reports to determine whether the iSTAR reports were reviewed by the school principals, a designee (i.e., assistant principal, school administrative assistant, and school dean), local district or Region staff, or central offices. Our review found that the school principal, a designee (i.e., assistant principal, school administrative assistant, and school dean), local district or regional staff, and/or central office administrator or staff reviewed or submitted 114 or 98% of the 116 reports we tested. The remaining two, or 2% of the 116 reports, were created in iSTAR but were not submitted for review. Table 10 below summarizes the results of our testing.

We also tested the 114 submitted reports to determine whether they were all reviewed by the school principal in iSTAR. Table 9 below summarizes the results of our testing.

---

[32] Bulletin 5269.2 Incident System Tracking Accountability Report (iSTAR), July 10, 2013, page 1.
[33] Bulletin 5269.3 Incident System Tracking Accountability Report (iSTAR), June 20, 2022, page 1.
[34] Ibid.
[35] The sample of 60 schools was comprised of a judgmental sample of 12 schools in each region and included at least one elementary school, one middle school, and one high school.
[36] iSTAR Annual Report 2021-2022.
[37] iSTAR Annual Report 2022-2023.
[38] The iSTAR activity history for each incident report captures the creator of the iSTAR incident report and all users who have viewed or updated the iSTAR report.

Table 9
Results of Testing
Statistical Random Sample of Submitted iSTAR Reports
July 1, 2021 to December 31, 2022

No. of Submitted iSTAR Reports	Percentage of iSTAR Reports Tested	Description of Finding
57	49%	The iSTAR report was viewed or submitted by the school principal.
57	49%	The iSTAR report was reviewed or submitted by a designee, Region staff, or central office personnel.
2	2%	The iSTAR report was not submitted for review.

AUDIT TEAM

This audit was conducted by the Office of the Inspector General's Audit Unit team:

Kathy Monishi, Audit Manager
Maria Thomas, Audit Manager
Armando Ng, Principal Auditor

ATTACHMENT A

VERBATIM RESPONSE TO THE DRAFT REPORT

FROM

THE DIVISION OF SCHOOL OPERATIONS

Alberto M. Carvalho
Superintendent

Pedro Salcido
Deputy Superintendent
Business Services & Operations

Andrés E. Chait
Chief of School Operations

Los Angeles Unified School District
Division of School Operations

333 S. Beaudry Avenue, 23rd Floor
Los Angeles, California 90017
Phone (213) 241-5337

September 24, 2025

iSTAR Audit Response

Thank you to the Office of the Inspector General for sharing their findings from the ISTAR audit conducted by their office. It is important to note that the ISTAR information reviewed by the OIG dates back to 2023. Accordingly, the data considered by the OIG may not reflect the most up to date information and current processes that govern the ISTAR protocols. Separate and apart from any findings by the OIG, DSO has already undertaken, over the last 2-3 years, comprehensive steps to address any issues with user access, training, etc.

Nonetheless, we welcome the feedback from the OIG and will continue to implement their recommendations as noted below.

Recommendations that the Division of School Operations (DSO) should:

Recommendation No. 1: Work with Information Technology Services (ITS), schools, and offices to complete a comprehensive review of all iSTAR users' privileges to ensure their access rights and user roles are aligned with their job duties.

Agree: DSO has continued to work with ITS to complete a comprehensive review of all iSTAR users' privileges annually to align their job duties. (On-going)

Recommendation No. 2: Work with ITS to implement periodic reviews of all iSTAR users and their access privileges (at least annually) for general users and semi-annually for privileged users. Operations stated that they had performed reviews of user access following our audit and identified approximately 1,800 users that should be deactivated. OIG obtained access to iSTAR and independently validated that 1,762 user accounts were deactivated.

Agree: DSO has implemented a system in place with ITS to periodically review an iSTAR user list annually. DSO will continue this process. (Frequency - **Annually**)

Recommendation No. 3: Revise the access permission process to include a secondary review from a different administrator, Operations Coordinator (OC), or higher-level authority.

Disagree: DSO has always implemented a system that includes a secondary review. Region and central office requests are reviewed by Division Leadership and Region-Administrators of Operations, then

submitted to the Division of School Operations leadership for review and approval as a higher level of authority. (Frequency -**On-going**)

Recommendation No. 4: Work with ITS to complete a review of the iSTAR security configuration, the access types, access sites, and user roles to ensure the least privileged access is granted to users. If necessary, reconfigure or add an additional level of security, delete, revise, or create new access types, sites, and user roles.

Agree: DSO has collaborated with ITS and will continue to work with them to review access requests and roles. Revisions to the iSTAR policy bulletin are currently being developed to provide additional guidance on the access levels that can be assigned by school site administrators. The guidance will outline the level of access for a user based on the role held in the District. (**On-going**)

Recommendation No. 5: Create a training program (in-person or virtual) for administrators about access permission, the existence of job aids, the importance of role-based access controls, and the risks of granting excessive access privileges.

Disagree: DSO has been providing virtual training annually during the summer, fall, and spring. This training will continue to be offered to all users on access permission, the existence of job aids, the importance of role-based access controls, and the risks of granting excessive access privileges. (On going - **Monthly**)

Recommendation No. 6: Program iSTAR to automatically align access type, site access, and user role assignments with Human Resources data, ensuring access privileges are updated for employees no longer assigned to the site and reducing the possibility of human error and oversight.

Disagree: Due to the variance of access by user role, the Region Administrators of Operations and Central office requests are currently reviewed by Division leadership and approved prior to review of DSO leadership. The layers of approval allow for access to be evaluated and approved based on the personalized role held by the requested employee. DSO is collaborating with ITS to assess the feasibility of utilizing OneAccess. Roles are assigned and aligned by DSO leadership. (**On-going**)

Recommendation No. 7: Work with the administrators and Region Administrators of Operations (AOOs) to reinforce District policy that all required incidents are submitted and issue types are reported in iSTAR.

Agree: DSO currently has a process in place to provide monthly training reminders and reports to Region AOOs and Operation Coordinators with iSTAR system reminders to be shared with school leaders. DSO is working with the iSTAR developers to send automatic monthly notifications. (**November 2025**)

Recommendation No. 8: Work with the Human Resources Division to implement a virtual training program detailing the iSTAR reporting requirements, the required incidents, and issue types. The virtual training should be required to be completed by all District staff annually.

Disagree: DSO provides ongoing virtual training annually during the summer, fall and spring. This training will continue to be offered to all users. (On-going **Monthly**)

Recommendation No. 9: Develop detailed guidance or job aids for submitting incidents and the issue type(s) that must be reported in iSTAR, required updates, examples of action plans, and proper resolution of incidents. A link to the guidance or job aids should be included in iSTAR for accessibility.

Disagree: Since the inception of iSTAR, DSO has provided job aids for submitting incidents, updating issue type(s) that must be reported in iSTAR. Additional job aids will be part of the updated iSTAR bulletin to provide more guidance for all users. **(On-going)**

Recommendation No. 10: Require administrators and AOOs to monitor iSTAR and certify periodically that all required incidents were submitted, submitted timely, included all applicable issue types, were updated regarding progress, action plan(s), and resolution, and closed when resolved.

Agree: Administrators and AOOs currently monitor iSTAR's and reports, work closely with site administrators to verify that incidents are submitted, updated and closed. In addition, error reports are sent frequently to Region Operations to follow up with schools. Monitoring of incidents will be automated to inform school principals of pending iSTAR's that need to be closed.
(Monthly)

Recommendation No. 11: Develop metrics to monitor incidents and resources to ensure incidents are addressed effectively and in a timely manner.

Agree: Administrators and AOOs currently monitor iSTAR's and reports, work closely with site administrators to verify that incidents are submitted, updated and closed. In addition, error reports are sent frequently to Region Operations to follow up with schools. Monitoring of incidents will be automated to inform school principals of pending iSTAR's that need to be closed.
(Monthly)

Recommendation No. 12: Work with the system owners of other District applications to develop system interfaces that automatically populate incidents in iSTAR, increasing efficiency and.

Disagree: This is not feasible as the iSTAR platform is unique and may require personalized information to address critical incidents. Additionally, the system was designed to provide Attorney-Client privilege as a confidential platform.

Recommendation No. 14: Work with the administrators and Region AOOs to provide updates for reported incidents, ensure action plan(s) and resolution(s) are documented, and close reports for incidents that have been resolved. Configure the iSTAR system to include automatic notifications when incidents have been open for more than a certain number of days, or when the incident information is incomplete.

Agree: DSO currently has a system in place to work with Region AOOs to review iSTAR error reports. The reports are shared frequently along with providing monthly professional development guidance on iSTAR's during DSO meetings. In addition, error reports are sent frequently to Region Operations to follow up with schools. Monitoring of incidents will be automated to inform school principals of pending iSTAR's that need to be closed. **(November 2025)**

Recommendation No. 15: Include required updates, documentation of action plans and resolutions, and examples of incidents considered closed as part of the training program.

Agree: DSO will continue to offer trainings that provide guidance on how to create and resolve incidents. Training will continue to be offered by DSO. Conversation about legal documentation will be discussed with OGC. **(On-going)**

APPENDIX 1

SCOPE AND OBJECTIVES, METHODOLOGY

SCOPE AND OBJECTIVES

The objectives of the audit were to determine whether (1) user access to iSTAR was appropriate, (2) incidents were reported in iSTAR and in a timely manner, (3) incidents were updated in iSTAR, including the resolution of the incidents, (4) the automatic email notifications to various departments, offices and divisions were working as intended, and (5) schools and non-school sites were monitoring the iSTAR incidents.

We conducted our audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions on our audit objectives. The audit covered the period from July 1, 2021 to December 31, 2022.

The audit team conducted the audit from November 8, 2022 to October 20, 2023.

METHODOLOGY

To accomplish our audit objectives, the audit team (i) researched pertinent District bulletins detailing policies and procedures relevant to iSTAR; (ii) conducted internal control questionnaires, interviewed and completed walkthroughs of iSTAR processes with key personnel within Operations; (iii) obtained a report of all iSTAR users and their access privileges; (iv) reviewed a sample of users to determine if their assigned access privileges and user roles were appropriate; (v) obtained a report of all incidents reported in iSTAR for the fiscal year 2021-2022 and the first six months of the fiscal year 2022-2023; (vi) reviewed a statistical random sample of reported incidents from 119 schools to determine whether incidents were reported timely, updates were provided, action plans and resolution were documented, and were reviewed by the administrators and AOs; (vii) obtained a report of all nursing and direct school mental health services provided to students for the first six months of the fiscal year 2022-2023; (viii) obtained a report of reported incidents, cases and employee misconduct from the Transportation Services Division, Los Angeles School Police Department and Staff Relations for the first six months of the fiscal year 2022-2023; (ix) obtained a report of facilities service requests from Facilities Maintenance and Operations for the first six months of the fiscal year 2022-2023; (x) reviewed all reports to identify incidents requiring the filing of an iSTAR report to determine whether a report was filed; (xi) received automated email notifications of submitted iSTAR reports for a period of time to verify that the iSTAR automated email notification functionality was working as intended; and (xii) visited a sample of 60 schools and interviewed the school administrators, the AOs for Region East, West, North and South, and the Director of the Transportation Services Division.

EVALUATION OF INTERNAL CONTROLS

In accordance with *Government Auditing Standards*, we obtained an understanding of internal control that is significant within the context of the audit objectives. We assessed whether internal controls were properly designed and implemented. For those controls that were deemed significant, we obtained sufficient, appropriate evidence to support our assessment of the effectiveness of those controls.

We are required to report deficiencies in internal controls that are significant within the context of the audit objectives. A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct (i) impairments of effectiveness or efficiency of operations, (ii) misstatements in financial or performance information; or (iii) noncompliance with provisions of laws, regulations, contracts, or grant agreements on a timely basis. Based on our audit, we did not find significant deficiencies in internal controls. Still, we found that internal controls could be strengthened and improved, details of which were provided in this report's Results of Audit section.

APPENDIX 2

DEFINITIONS OF CURRENT ISSUE TYPES

INCIDENT SYSTEM TRACKING ACCOUNTABILITY REPORT (iSTAR)

Issue Types	Definition
Abduction	Every person who forcibly, or by any other means of instilling fear, steals or takes, or holds, detains, or arrests any person in this state, and carries the person into another country, state, or county, or another part of the same county, is guilty of kidnapping.
Accident	An unforeseen and unplanned event or circumstances.
Altercation	Angry or heated argument or quarrel (not physical).
Arrest	Taking a person into custody, in a case, and in the manner authorized by law. An arrest may be made by a peace officer or by a private person.
Bullying	Any persistent, severe, or pervasive physical or verbal act or conduct, including electronic communications, and including one or more acts committed by a pupil or group of pupils, directed toward one or more pupils that have or can be reasonably predicted to have one or more of the following effects on a reasonable pupil: 1. Reasonable fear of harm to a person or property of pupil(s). 2. Substantially detrimental effect on the physical or mental health of pupil(s). 3. Substantial interference with academic performance. 4. Substantial interference with the ability to participate in or benefit from school services, activities, or privileges. Cyberbullying – Bullying is by electronic act, which includes transmission of a communication by text, sound, social network activity, image, video, message, post on a website, or other form of communication sent by an electronic device. Indirect – The use of intimidation or peer pressure to cause harm to a third party(ies). Nonverbal – The use of threatening gestures, staring, stalking, graffiti or graphic images, or destruction of property to cause distress, intimidation, discomfort, pain, or humiliation. Physical – The intentional, unwelcome act of beating, biting, fighting, hitting, kicking, poking, punching, pushing, shoving, spitting, or tripping. Social – Spreading rumors, manipulating relationships, exclusion, blackmailing, isolation, rejecting, using peer pressure, or ranking personal characteristics.

Issue Types	Definition
	Verbal – Hurtful gossiping, making rude noises, name-calling, spreading rumors, or teasing.
Burglary	Any entry of a building with the intent to commit a theft or felony.
Child Annoyance	An act of irritating or distracting. It is a source of vexation or nuisance by an adult toward a minor.
Custody Issue	The right of guardianship, care, control, and maintenance of a child, especially such a right granted by a court.
Death	The permanent cessation of all vital bodily functions. Death must be confirmed. The deceased must be a current employee or student.
Discrimination/ Harassment	Discrimination is different treatment on the basis of a protected category in the context of an educational program or activity, without a legitimate, nondiscriminatory reason, that interferes with or limits the ability to participate in or benefit from the services, activities, or privileges provided by the District. Harassment is: 1. A target was subjected to unwelcome conduct related to a protected category. 2. The harassment was subjectively offensive to the target. Discriminatory – Harassment or Hostile – Environment Harassment: 1. A target was subjected to unwelcome conduct related to a protected category. 2. The harassment was subjectively offensive to the target. 3. The harassment would be offensive to a reasonable person of the same age and characteristics in the same circumstances. 4. The harassment was sufficiently severe, pervasive, or persistent. 5. As to interfere with or limit a student's ability to participate in or benefit from the District's services, activities, or opportunities offered. Sexual harassment – Unwelcome sexual advances, requests for sexual favors, and other verbal, visual, or physical conduct of a sexual nature, made by someone from or in the work or educational setting under any of the following conditions: 1. Submission to the conduct is explicitly or implicitly made a term or a condition of an individual's employment, academic status, or progress. 2. Submission to, or rejection of, the conduct by the individual is used as the basis of employment or academic decisions affecting the individual. 3. The conduct has the purpose or effect of having a negative impact upon the individual's work or academic performance, or of creating an intimidating, hostile, or offensive work or educational environment. 4. Submission to, or rejection of, the conduct by the individual is used as the basis for any decision affecting the individual regarding benefits and services, honors, programs, or activities available at or through the educational institution.

Issue Types	Definition
	Disability: 1. A physical or mental impairment that substantially limits one or more of the major life activities of such individual; 2. A record of such an impairment; or 3. being regarded as having such an impairment. Gender/Sex: 1. A person's actual or perceived sex and includes a person's gender identity and gender expression. (EC 210.7) Gender includes male, female, non-binary, and transgender. 2. Gender expression – a person's gender-related appearance and behavior, whether or not stereotypically associated with the person's assigned sex at birth. (EC 210.7). 3. Gender Identity – A person's gender-related identity, appearance, or behavior, whether or not different from that traditionally associated with the person's physiology or assigned sex at birth. 4. Race/Color/Ethnicity/Nationality – Includes ancestry, color, ethnic group identification, ethnic background, citizenship, country of origin, and national origin. (EC sections 212, 212.1). 5. Religion – Includes all aspects of religious belief, observance, and practice, and includes agnosticism and atheism. (EC 212.3.) 6. Sex Orientation – It means heterosexuality, homosexuality, and bisexuality, though commonly used terms include, but are not limited to, heterosexual, lesbian, gay, asexual, and bisexual.
Disrupted Online Learning Sessions	Disrupted Online Learning Sessions.
Disrupted School Operations	Egregious disorderly conduct or act of troubling, or annoying someone, or disrupting school-site/District programs or activities.
Fighting / Physical Aggression	1. Any person who unlawfully fights in a public place or challenges another person in a public place to fight. 2. Any person who maliciously and willfully disturbs another person by loud and unreasonable noise. Any person who uses offensive words in a public place which are inherently likely to provoke an immediate violent reaction.
Fraud	An intentional deception made for personal gain or to damage another individual, District property, or activity.
Hate Crime	A criminal act (threat, injury, use of force, damage, or destruction of property) committed in whole or in part because of one or more actual or perceived characteristics of the victim(s): disability; gender, nationality; race or ethnicity; religion; sexual orientation; association with a person or group with one or more of these actual or perceived characteristics.
Hazing	A method of initiation or pre-initiation into a pupil organization or body, whether or not the organization or body is officially recognized by an

Issue Types	Definition
	educational institution, which is likely to cause serious bodily injury or personal degradation or disgrace resulting in physical or mental harm to a former, current, or prospective pupil. For purposes of this subdivision, "hazing" does not include athletic events or school-sanctioned events.
Illegal/ Controlled Substance	Possession or use of illegal drugs, including alcohol, tobacco, and other intoxicants, on campus and at school activities. Marijuana: - Edible Food Item - Prescription - Non-prescription under one ounce - Non-prescription over one ounce.
Inappropriate Conduct (Employee as suspect only)	Inappropriate sexual or non-sexual incidents involving an employee; employee-to-employee, employee-to-other adults.
Inappropriate Conduct Non-Sexual (employee as suspect only and student as victim)	Inappropriate sexual or non-sexual incidents involving an employee; employee-to-student misconduct.
Inappropriate Conduct Sexual (employee as suspect only and student as victim)	Inappropriate sexual or non-sexual incidents involving an employee; employee-to-student misconduct.
Intergroup Conflict	A conflict that occurs between two or more persons representing different groups. Group identity may be defined as a source of pride, self-esteem, and belonging based on shared traits such as race, ethnicity, culture, gang/crew association, religion, political ideology, or other socially defined commonality.
Lockdown	To keep students in a designated, secured location on campus in order to provide a greater level of protection or as a security measure.
Loitering	To stand idly about; linger aimlessly.
Medical	Events requiring treatment or medical attention, such as asthma, fainting, chest pain, intoxication, illness, diabetes, seizure, shock, etc.
Missing/ Runaway	A disappearance of a person, which is possibly not voluntary, or a person whose whereabouts are unknown.
Natural/Man Made Disaster	A disaster is a sudden calamitous event with significantly disruptive or destructive consequences. Disasters can be caused by naturally occurring events (such as an earthquake, landslide, or tsunami), or human-caused events, either accidental (such as a toxic spill or mass vehicle crash), or deliberate (such as a terrorist attack or sabotage).
Public Shelter	The use of a school facility by the American Red Cross to temporarily care for members of the public displaced by a disaster.
Robbery/ Extortion	Felonious taking of personal property in the possession of another, from his person or immediate presence, and against his will, accomplished by means of force or fear (different than burglary).

Issue Types	Definition
Sex Crime/ Sexual Behavior	Sex Crime/Sexual Behavior-Inappropriate – Inappropriate sexual behavior or sexual practices or sexual activities refers to the manner in which humans experience and express their sexuality. Physical – Includes rape, incest, sexual relations with children (pedophilia), possession of child pornography, voyeurism (Peeping Tom), exhibitionism, and other inappropriate physical sexual behavior. Verbal – Obscene phone calls, explicit sexual propositions, sexual innuendos, and other verbal behavior of a sexual nature.
Shooting	Any discharge of a firearm.
Suicide Risk	A Risk Assessment Referral Data (RARD) report must be completed if the incident is centered around or involves the behavior of a student. Suicidal Ideation/behavior (non-injury) – Any observable behavior or communication (e.g., verbal, written, drawing) that may indicate an individual's intent to die by suicide, the presence of a plan to die, and/or the means to carry out one's plan to die, the behavior/ideation does not result in physical injury to the individual. Self-Injury/Cutting – The deliberate act of harming one's own body, through means such as cutting or burning; indicators include frequent or unexplained scars, cuts, or burns, bruises on the neck, headaches, red eyes, ropes/ties/belts/ as a sign of the "choking game"; possession of sharp objects; and evidence of self-injury in drawings, journals, pictures, or social networking sites. Suicidal Behavior (injury) – Any observable or communication (e.g., verbal, written, drawing) that may indicate an individual's intent to die by suicide, the presence of a plan to die, and/or the means to carry out one's plan to die, the behavior results in physical injury to the individual.
Theft	Every person who shall feloniously steal, take, carry, lead, or drive away the personal property of another, or who shall fraudulently appropriate property which has been entrusted to him or her, or who shall knowingly and designedly, by any false or fraudulent representation or pretense, defraud any other person of money, labor, or real or personal property, or who causes or procures others to report falsely of his or her wealth or mercantile character and by thus imposing upon any person, obtains credit and thereby fraudulently gets or obtains possession of money, or property, or obtains the labor, or service of another, is guilty of theft.
Threat	A Risk Assessment Referral Data (RARD) report must be completed if the incident is centered around or involves the behavior of a student. Threatened to cause physical injury to another person – An expression of an intention to injure another person. A threat may be direct,

Issue Types	Definition
	indirect, verbal, non-verbal, written, or electronic and may target an individual, a particular group on campus, the entire school, or the community. Attempted physical injury to another person – A willful attempt to inflict harm that could likely result in death, bodily injury, physical damage to property, or disruption to institutions, or District-sponsored activities. Caused physical injury to another person – Willfully inflicts harm that would likely result in death or bodily injury. The physical injury may require professional medical treatment, including that from a school nurse. Terroristic Threat – Any person who willfully makes a statement that threatens to kill or cause great bodily injury to another person. 1. The statement is communicated (e.g., verbally, in writing, by means of electronic communication) to the victim and intended to be understood as a threat to said victim; the statement is clear, unconditional, and specific. 2. Even if there is no intent of actually carrying it out, it is communicated with the intent that the threat was to be carried out immediately, and the person making the threat has the ability (means) to carry out the threat and the threatening statement causes the victim to be in reasonable fear for his or her own safety or the safety of his or her immediate family. 5585 (Minor)/5150 (Adult) Hospitalization – The involuntary detention of an individual for assessment and evaluation, who, as a result of a mental disorder, is determined to be a danger to themselves or others.
Trauma/ Violence Exposure	Experiences that threaten life or physical integrity that overwhelm one's capacity to cope, tending to evoke feelings of fear and helplessness. Community Violence: 1. Witnessing or experiencing severe violence, experiencing a severe motor vehicle accident, house fire, or being physically injured. 2. Familial Violence – witnessing or experiencing domestic disputes and/or violence that occurs in the home between family members. Grief/Loss/Death: 1. Includes the sudden loss of a loved one, generally as a result of sudden onset illness, violence, or suicide. 2. Sudden severe illness of self or loved one.
Trespass	An unlawful intrusion.

Issue Types	Definition
Utility Failure	The full or partial loss of a utility such as power or water on site: Power Outage – The full or partial loss of electrical power to the site. Water Outage – The full or partial loss of water supply to the site.
Walkout/ Demonstration	The action of leaving campus or office without administrative consent in order to express disapproval.
Weapons	Any person, except a duly appointed peace officer as defined in Penal Code 626.10, who brings or possesses any dirk, dagger, ice pick, knife having a blade longer than 2 1/2 inches, folding knife with a blade that locks into place, razor with an unguarded blade, taser, or stun gun. Weapon – Any instrument which is used in a threatening manner against another person with the intent and the ability to cause great bodily injury. Such objects may include but are not limited to, guns, knives (having a blade longer than 2 1/2 inches), rocks, screwdrivers, or scissors.

APPENDIX 3

Table 10 below summarizes the number of OCs, the number of schools ranked with the highest or high SENI score, the number of students enrolled in the regions, the number of iSTAR reports, and the number of iSTAR issue types.

The number of schools, the number of schools ranked with the highest and high SENI, and the unduplicated student count[39] were obtained from the District Fiscal Year 2023-2024 SENI Allocation Summary.[40] The enrollment count was obtained from the District Fiscal Year 2023-2024 Title I Ranking,[41] and the reported number of incidents and issues from the Fiscal Year 2022-2023 iSTAR Annual Report.[42]

Table 10
District Region
Regional Operations Coordinator

District Region	No. of Operations Coordinators	No. of Schools	No. of Schools Ranked With the Highest/ High SENI	Student Enrollment Count	Unduplicated Student Count	No. of iSTAR Reports	No. of iSTAR Issue Types
East	7	221	109	111,555	106,485	13,961	15,938
West	6	145	24	66,106	47,166	8,592	10,064
North	7	229	56	132,253	103,935	15,422	17,905
South	6	183	95	93,304	86,835	10,669	12,364

Table 11 below illustrates the average number of schools, schools ranked with the highest and high SENI, student enrollment, unduplicated students, iSTAR reports, and iSTAR issue types per Regional OC by region.

Table 11
Average Per Regional Operations Coordinator
By Region

District Region	Average No. of Schools Per Operations Coordinator	Average No. of Schools Ranked With The Highest and High SENI Per Operations Coordinator	Average Number of Students Enrolled Per Operations Coordinator	Average Number of Unduplicated Students Per Operations Coordinator	Average Number of iSTAR Reports Per Operations Coordinator	Average Number of iSTAR Issue Types Per Operations Coordinator
East	32	16	15,936	15,212	1,994	2,277
West	24	4	11,018	7,861	1,432	1,677
North	33	8	18,893	14,848	2,203	2,558
South	31	16	15,551	14,473	1,778	2,061

[39]Unduplicated student count means each pupil is counted once, and is an English learner, meets income or categorical eligibility requirements for free or reduced-price meals under the National School Lunch Program, or is a foster youth.
[40]Fiscal Year 2023-2024 SENI Allocation Summary.
[41]Fiscal Year 2023-2024 Title I Ranking.
[42]iSTAR Annual Report 2022-2023.

APPENDIX 4

Division/Department Applications
July 1, 2022 to December 31, 2022

Division/ Department Name	Application Name	Description
District Nursing Services (DNS)	Welligent.net	Tracks visits to the nurse's office and services rendered by the school nurse(s). Incidents and services include but are not limited to health assessments, screenings, athletic and other school injuries, illness, medical treatments, and the administering of medications prescribed by a physician.
School Mental Health (SMH)	Welligent.com	Tracks mental health services provided to students. The mental health services include but are not limited to mental health awareness, suicide risk assessment, behavioral management, violence prevention and empathy skills, classroom consultation, and student counseling.
Facilities Maintenance and Operations (M&O)	MAXIMO	Manages maintenance and operations' service requests that include property damage, vandalism, theft, utility failure, and graffiti removal
Los Angeles School Police Department (LASPD)	Records Management System (RMS) and Computer-aided Dispatching (CAD)	Manages calls received and cases worked by school police staff. Cases include but are not limited to battery, assault, vandalism, burglary, sex offense, weapons, and drug abuse.
Transportation Services Division (TSD)	BusOps	Records events that occurred during the bus routes. Events include, but are not limited to, injuries on the buses, vandalism, theft, car accidents, and misconduct.
Staff Relations (SR)	CASE	Manages cases of employee misconduct, including disciplinary actions taken, if any. However, SR provided the audit team with Excel spreadsheets listing cases involving employee misconduct with the TSD, Facilities Services Division, Certificated employees, and ITS. We did not receive cases involving the Food Services Division and other Classified central office employees.

OIG HOTLINE

Office of the Inspector General
"Independent and Objective Oversight"

REPORT FRAUD, WASTE AND ABUSE

(213) 241-7778 or (866) 528-7364

inspector.general@lausd.net

https://www.lausd.org/oig

- ❑ Misuse of LAUSD funds and resources
- ❑ Retaliation for reporting misconduct
- ❑ Anyone can make a report
- ❑ You may remain anonymous

English

Español