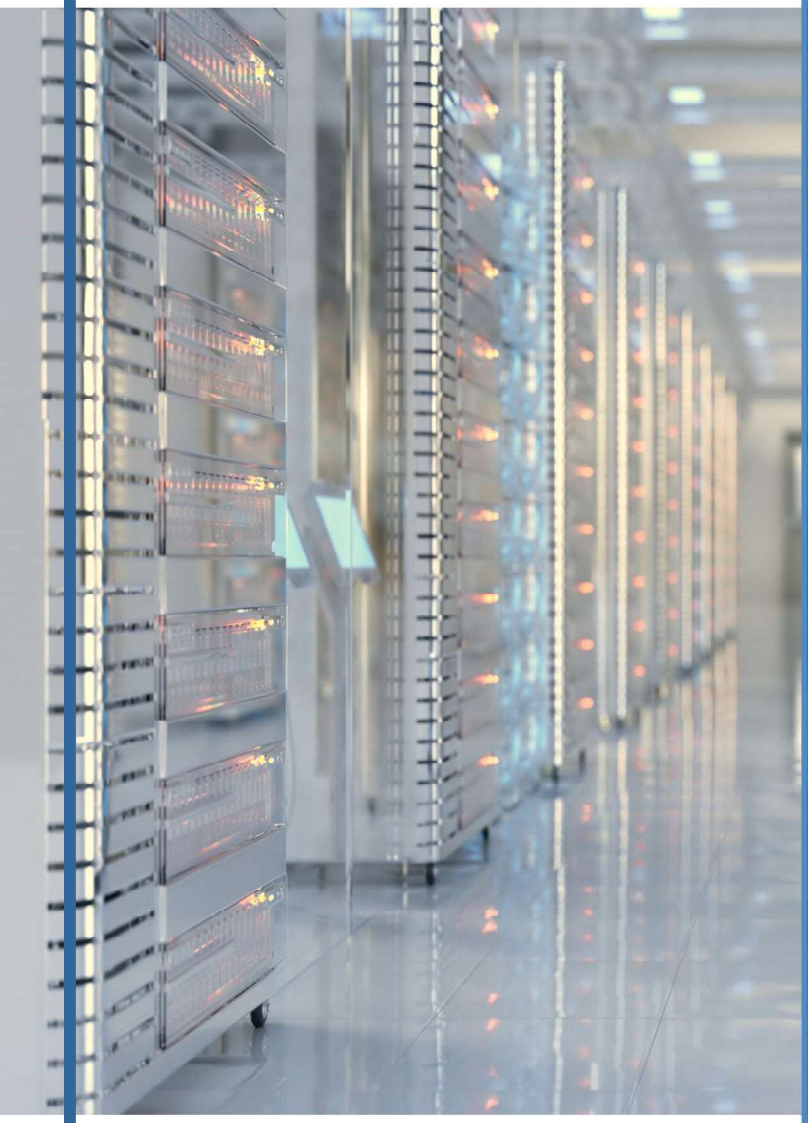
Los Angeles Unified School District
Office of the Inspector General



Follow Up Audit of the Information Security Audit

OA 25-1459
August 6, 2025

Sue Stengel
Inspector General

Los Angeles Unified School District
Office of the Inspector General

August 6, 2025

Mr. Soheil Katal, Chief Information Officer
Information Technology Services
Los Angeles Unified School District
333 S. Beaudry Avenue, 10th Floor
Los Angeles, CA 90017

RE: Follow-Up Audit of the Information Security Audit

Dear Mr. Katal,

This is a redacted copy of the final report on the Follow-Up Audit of the Information Security Audit of the Los Angeles Unified School District (District) Information Technology Services. Crowe, LLP, a subject matter expert in cybersecurity, conducted the engagement.

The report contains an abbreviated summary of the results of the engagement to follow up on the status of implementation and corrective actions from the September 2020 cybersecurity audit and perform internal and external penetration testing assessments.

Due to the sensitive nature of the findings from the audit, the OIG has redacted the findings in the full report provided to ITS under a separate cover. While the OIG has a responsibility to make sure certain parties are informed of organizational risks, we balance this responsibility against the introduction of additional risk exposure through the disclosure of detailed reports.

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: 2025.08.06 12:42:08 -07'00'

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

Sue Stengel
Digitally signed by Sue Stengel
DN: cn=Sue Stengel, o=OIG, ou=OIG, email=susan.stengel1@lausd.net, c=US
Date: 2025.08.06 13:09:47 -07'00'

Sue Stengel, Esq., CIG
Inspector General

c. Richard Meraz, Michael Lee, Matthew Friedman, Jorge Ballardo, Cheri Thomas, Dana Greer

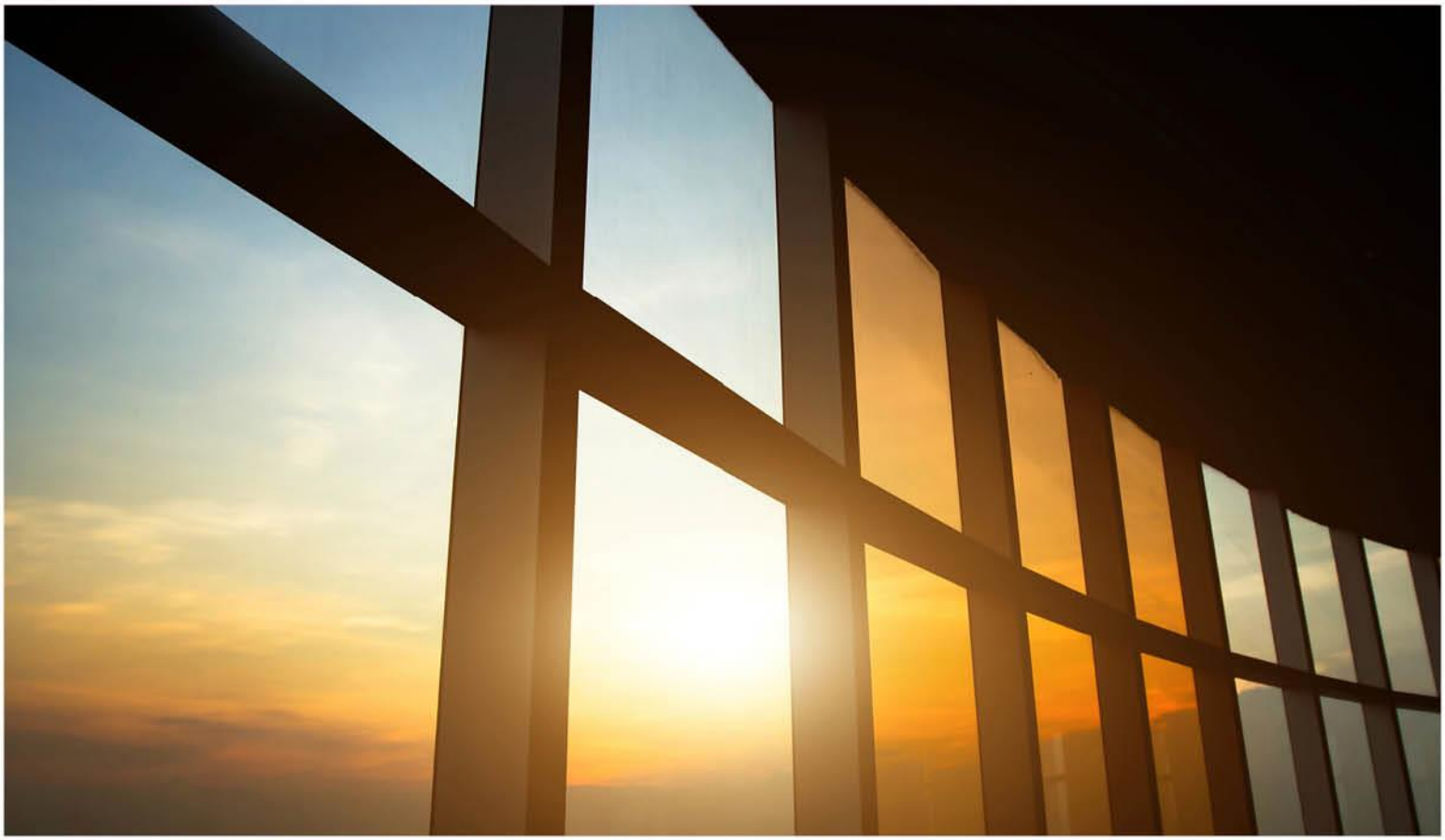
Crowe

Smart decisions. Lasting value.™

Los Angeles Unified School District

Performance Audit Report
Internal and External Penetration Assessment

February 2025



I. Executive Summary

Crowe LLP (Crowe) performed an Internal and External Penetration Assessment and updated NIST Assessment for Los Angeles Unified School District (LAUSD) during the weeks of January 6, 2025 to January 27, 2025. The goal of the assessment was to perform a follow up of the Cybersecurity Assessment performed by Crowe in September 2020.

Overview

The overall objective of the engagement was to update the September 2020 Cybersecurity Assessment, including internal and external penetration testing.

The goal of the penetration testing was to assess the ability of the LAUSD network to resist attacks from internal threats as well as from the Internet and other external sources. Crowe identified LAUSD systems and services that were accessible on the LAUSD internal network and from the Internet. Crowe then attempted to identify and verify vulnerabilities that could allow an attacker to gain access to LAUSD internal network, gain elevated access, or to gain access to sensitive information.

An assessment of the LAUSD Internet address ranges identified fifty-three targets, including twenty-nine web services as well as four remote access services and four internet phone services. LAUSD hosts all these devices and Crowe targeted them during the External Penetration Assessment.

The assessment of the LAUSD internal network identified approximately 7000 devices, including workstations, servers, and networking devices which are hosted internally by LAUSD. Crowe targeted these devices during the Internal Penetration Assessment.

LAUSD's Information Technology staff had to add the assessment device to an allow list in the organization's security controls for Crowe to perform the internal testing. Additionally, the LAUSD staff detected some of Crowe's activities during the technical portion of the assessment. LAUSD did not block Crowe's network access to allow Crowe to fully identify vulnerabilities that may be present.

This is the second Penetration Assessment performed for LAUSD by Crowe.

Project Methodology & Approach

All controls were assessed based upon the scope approved by LAUSD, which covered the District's information systems and applications. The following steps represent the actions performed to deliver the assessment:

1. **Phase One – Project Planning and Kickoff**
   During Phase One, an information request list was submitted to gather existing policies and procedures. Additionally, a kickoff meeting was held to discuss the project timeline and expectations. Interviews were scheduled for information-gathering sessions with both business and IT management.

2. **Phase Two – Assessment**
   An assessment of information security controls was performed to obtain an understanding of the environment. Numerous interviews were conducted with Management from a cross-section of departments throughout the District, as well as with Information Technology (IT) subject matter experts. Crowe performed penetration testing and reviewed technical configuration of systems within the environment.

3. **Phase Three – Project Deliverables**
   Detailed results and accompanying recommendations from fieldwork are documented in this report.

Reporting Methodology

In this report, we provide a summary of our results and recommendations as well as management's responses. To assist you in analyzing our recommendations, we have provided our suggestions for corrective action based on the finding's exposure to loss or increased regulatory scrutiny, as follows:

High – Requires immediate remedy and, if left uncorrected, exposes LAUSD to significant or immediate risk of loss, asset misappropriation, data compromise or interruption, fines and penalties, or increased regulatory scrutiny.

Moderate – Requires timely remedy and, if left uncorrected, may expose LAUSD to risk of loss or misappropriation of District assets, compromise of data, fines and penalties, or increased regulatory scrutiny. These issues should be resolved in a timely manner, but after any high priority issues.

Low – Should be addressed as time and resources permit. While it is not considered to represent significant or immediate risk, repeated oversights without corrective action or compensating controls could lead to increased exposure or scrutiny.

Summary of Results

The table below displays the number of recommendations identified through the procedures performed, categorized by priority.

Area of Assessment	High	Moderate	Low
Internal Penetration			
Windows and Active Directory System Security	-	-	4
Network Architecture and Infrastructure Management	-	1	4
Patch Management	-	-	2
Database Security	-	-	-
Email Architecture Security	-	-	-
Unix and Linux System Security	-	-	-
Web Application Security	-	-	-
Printers and Multi-function Devices	-	-	-

Area of Assessment	High	Moderate	Low
Data Storage and Access Controls	-	-	2
External Penetration			
Web Application Security	-	-	1
Data Storage and Access Controls	-	-	-
Patch Management	-	-	1
Identify External Targets	-	-	-
Network Architecture and Infrastructure Management	-	-	-
Total	-	1	14
Repeat Finding	-	-	1
Recurring Issue	-	1	7

The most significant risk identified during our assessment was identified in the following area:

- Network Segmentation

In addition to the item summarized here, Crowe noted other items that do not represent significant risk at this time but offer opportunities for LAUSD to further strengthen controls and processes. Crowe also identified various controls that were successfully mitigating information security risks for the District.

Information security is an ongoing process and Internal and External Penetration Assessments cannot guarantee the security of a network. Since new vulnerabilities are discovered daily, LAUSD should continue with ongoing security assessments.

Crowe would like to thank LAUSD for this opportunity to report the results of this assessment and to thank LAUSD's personnel for their cooperation and assistance.

II. Summary of Scope

Crowe followed a structured assessment process to evaluate the security of the LAUSD internal and external network. The Crowe assessment team divided this process into the following phases:

IIIa. Internal Penetration Assessment

Phase 1: Internal Network Target Identification
- Passively monitor network traffic to identify active systems and subnets on the network.
- Perform ICMP scans to identify active systems and subnets on the network.
- Query internal DNS servers to identify IP addresses.
- Perform TCP and UDP port scans to identify available services on the LAUSD network.

Phase 2: Internal Network Security Assessment
- Probe identified services to determine target configuration and vulnerabilities.
- Verify all identified potential vulnerabilities.
- Attempt to gain access to LAUSD systems and sensitive information by exploiting vulnerabilities.

IIIb. External Penetration Assessment

Phase 3: Target Identification
- Perform Internet searches and search registration data to identify domains and Internet Protocol (IP) ranges associated with LAUSD.
- Query domain name servers to identify additional IP addresses.
- Scan LAUSD-related IP address ranges to identify potential targets.

Phase 4: Internet Target Security Assessment
- Probe identified services to determine target configuration and vulnerabilities.
- Verify all identified potential vulnerabilities
- Attempt to gain access to LAUSD network and sensitive information by exploiting vulnerabilities.

Internet Target Scope
Crowe reviewed websites owned and operated by LAUSD.

For the identification and assessment of targets on the internal networks, Crowe was provided by LAUSD with valid credentials or with other access to LAUSD systems.

The specific procedures performed were based on the concepts of selective testing. Although Crowe's testing was performed in some areas without exception, Crowe can provide no assurance that exceptions would not have been detected had procedures been changed or expanded.

It should also be recognized that internal controls are designed to provide reasonable, but not absolute, assurance that errors and irregularities will not occur, and that procedures are performed in accordance with management's intentions. There are inherent limitations that should be recognized in considering the potential effectiveness of any system of internal controls. In the performance of most control procedures, errors can result from misunderstanding of instructions, mistakes in judgment, carelessness, or other factors. Internal control procedures can be circumvented intentionally by management with respect to the execution and recording of transactions, or with respect to the estimates and judgments required in the processing of data.

Controls may become ineffective due to newly identified business or technology exposures. Further, the projection of any evaluation of internal control to future periods is subject to the risk that the procedures may become inadequate because of changes in conditions, and that the degree of compliance with procedures may deteriorate.

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