INTRADEPARTMENTAL CORRESPONDENCE

November 25, 2025
1.0

BPC# 25-315

TO: The Honorable Board of Police Commissioners

FROM: Inspector General, Police Commission

SUBJECT: OFFICE OF THE INSPECTOR GENERAL'S REVIEW OF THE LOS ANGELES POLICE DEPARTMENT'S CONTROLS OVER ACCESSING AND SHARING CONFIDENTIAL INFORMATION IN SEXUAL ASSAULT INVESTIGATIONS

RECOMMENDED ACTION

REVIEW and APPROVE the Office of the Inspector General's (OIG's) Review of the Los Angeles Police Department's Controls Over Accessing and Sharing Confidential Information in Sexual Assault Investigations.

DISCUSSION

Following the high-profile case involving former Los Angeles Police Department (LAPD or Department) Commander Cory Palka and former CBS Chairman and CEO Les Moonves in late 2022, the Board of Police Commissioners requested that the OIG examine the Department's practices and procedures for handling investigations into crimes of sexual assault, with a specific focus on the security measures in place to safeguard investigative information. At the time, Moonves was accused of sexual assault, and reports indicated that both Palka and a detective—who was not in Palka's immediate chain of command—allegedly provided Moonves, a CBS senior vice president, and their legal counsel with confidential status updates on the Department's criminal sexual assault investigation of Moonves in 2017 and 2018.

The OIG's review examined Department policies and procedures to assess whether existing guidelines provide clear and enforceable standards for protecting confidential information. Additionally, the review evaluated Department databases used for documenting, tracking, and reporting investigative information, focusing on their security features, and user access controls. The attached report provides more information about the review's objectives and findings.

I am available to provide any further information the Commission may require.

MATTHEW J. BARRAGAN
Inspector General
Police Commission

Attachment

LOS ANGELES POLICE COMMISSION

REVIEW OF THE LOS ANGELES POLICE DEPARTMENT'S CONTROLS OVER ACCESSING AND SHARING CONFIDENTIAL INFORMATION IN SEXUAL ASSAULT INVESTIGATIONS

Conducted by the

OFFICE OF THE INSPECTOR GENERAL

Matthew J. Barragan

Inspector General

November 25, 2025

TABLE OF CONTENTS

REVIEW OF THE LOS ANGELES POLICE DEPARTMENT'S CONTROLS OVER ACCESSING AND SHARINGCONFIDENTIAL INFORMATION IN SEXUAL ASSAULT INVESTIGATIONS

I. BACKGROUND

Following the high-profile case involving former Los Angeles Police Department (LAPD or Department) Commander Cory Palka and former CBS Chairman and CEO Les Moonves in late 2022, the Board of Police Commissioners (BOPC or Police Commission) requested that the Office of the Inspector General (OIG) examine the Department's practices and procedures for handling investigations into crimes of sexual assault, with a specific focus on the security measures in place to safeguard investigative information. At the time, Moonves was accused of sexual assault, and reports indicated that both Palka and a detective—who was not in Palka's immediate chain of command—allegedly provided Moonves, a CBS senior vice president, and their legal counsel with confidential status updates on the Department's criminal sexual assault investigation of Moonves in 2017 and 2018.[1,2] Below are the findings from the OIG's review.

II. PURPOSE

The purpose of this limited-scope OIG review was to assess whether the Department's existing policies, procedures, and practices are sufficient to mitigate the risk of LAPD employees improperly accessing, obtaining, or sharing sensitive or confidential information with unauthorized individuals—whether within the Department or externally. This review specifically focused on information security measures rather than evaluating the Department's broader policies and procedures for conducting sexual assault investigations and identifying any gaps or vulnerabilities that may require policy or procedural changes.

III. METHODOLOGY

The OIG's review examined internal Department investigations and audits to determine whether and how past unauthorized disclosures and security concerns were identified and addressed. It also included an analysis of Department policies, procedural manuals, instructional guides, and other reference materials to assess whether existing guidelines provide clear and enforceable standards for protecting confidential information. The OIG also met with subject matter experts from Detective Bureau and Information Technology Bureau (ITB) to understand how investigative information is handled, stored, and accessed in practice. Additionally, the review evaluated Department databases and systems used for documenting, tracking, and reporting investigative information, focusing on their security features, user access controls, and audit capabilities.

---

[1] Although the detective was able to obtain some basic general information about the investigation of Moonves, he/she was not assigned to and involved in that investigation. The main information provided by the detective was that the Los Angeles District Attorney was extremely unlikely to prosecute the case because the two alleged sexual assaults occurred in 1986 and 1988 and were not reported to LAPD until November 2017, approximately 30 years later. Furthermore, there were no witnesses and physical evidence. Earlier, Palka had provided Moonves a copy of the November 2017 police report.

[2] Palka and the detective resigned from the LAPD in March 2021 and March 2020, respectively.

Through this multi-faceted approach, the OIG aimed to identify potential gaps in policy and procedures, as well as areas for improvement to ensure that investigative information is adequately protected from unauthorized access, misuse, or disclosure.

Specifically, the OIG's review entailed the following:

a) Examined LAPD Operations-West Bureau's (OWB's) review of the Moonves criminal sexual assault investigation, as well as 12 other criminal sexual assault investigations conducted by the Department between 2017 and 2019, some of which involved high-profile individuals.

b) Reviewed the internal misconduct investigation concerning Palka and the detective, including the disposition of all allegations and the rationales behind those determinations.[3]

c) Reviewed Department policies on confidentiality, information security, Criminal Offender Record Information (CORI), and the reporting and sharing of sex crime victim information.

d) Analyzed the Detective Manual, the Detective Case Tracking System (DCTS) Instructional Guide[4], and Record Management System (RMS) training and reference materials, focusing on the protocols for opening, securing, accessing, maintaining, and closing criminal investigative cases.

e) Prepared and distributed a detailed questionnaire to the Department, seeking information about the current policies, procedures, and internal controls designed to mitigate the risks of LAPD employees improperly accessing or sharing confidential sexual assault investigation information. The OIG then conducted a detailed review of the Department's responses.

[3] The general intent of this review was to understand the nature and disposition of the alleged employee misconduct. The intent was not to evaluate the adequacy or completeness of the complaint investigation and the reasonableness of the allegation dispositions.

[4] After the project was initiated and an initial draft report was completed and shared with the Department for review, the OIG was informed that the Department no longer uses DCTS. Any legacy data previously maintained in DCTS is now accessible through a database managed by a third-party vendor.

f) Received in-depth demonstrations of both RMS and DCTS.[5,6] These demonstrations covered general system usage, as well as specific procedures for opening cases, restricting access, entering and deleting digital documents, and managing access permissions for individual criminal cases.

IV. EXISTING DEPARTMENT SYSTEMS

Overview

In 2001, the Department implemented the DCTS – a system designed specifically for tracking criminal investigations from start to finish. In 2024, the Department replaced DCTS with the RMS – a system with multiple applications throughout the Department,[7] including an application for tracking criminal investigations. In addition to having a greater range of applications and modules for integration throughout the entire Department, RMS also improves the required reporting of crime data to the California Department of Justice (CalDOJ) and Federal Bureau of Investigation (FBI).[8]

DCTS

The Department used DCTS to track various aspects of its investigations, including detective or investigator assignments and major case activities. Technically, this was achieved within DCTS by structuring the system into divisions, units, and teams, with employees assigned to each group through the backend administrative infrastructure. The DCTS also incorporated "leveled access" controls as a security feature to protect sensitive information. These access levels determined who could use DCTS, what information they could view, and what actions they could take within the system. For non-confidential cases, any employees assigned to the same unit could add, create, or modify case notes. However, for confidential cases, only employees specifically

[5] Criminal cases were first entered into RMS for Operations-Central Bureau on March 7, 2024, with a phased rollout that eventually encompassed all four bureaus by May 31, 2024. Subsequently, by December 31, 2024, all criminal investigative divisions were using and entering new cases into RMS, with no new cases entered in DCTS.[5]

[6] In addition to being used internally for criminal cases, DCTS and RMS have collected arrest and other information required by the California Department of Justice per Penal Code §13010-13012 and 13020-13021. Also, this arrest and other information is reported monthly to the Federal Bureau of Investigation (FBI) per its Uniform Crime Reporting requirement.

[7] RMS is also widely used by the Office of Operations and Department patrol divisions, Custody Services Division, and Training Bureau.

[8] Per a Department Operations Center Notice to all LAPD employees on April 1, 2024, "The RMS is designed to enhance efficiency, transparency and effectiveness in serving our community. This new RMS also enables the LAPD to comply with the new standard for law enforcement criminal data reporting in the United States National Incident-Based Reporting System (NIBRS), mandated by the FBI."

assigned to the case—or those within their immediate chain of command—had permission to add, create, or modify case notes. As noted above, the Department no longer uses DCTS.

RMS

The RMS shares certain security features with DCTS, including restrictions on accessing case information. One key feature in RMS is the "secure folder" feature, which allows the lead investigator or their supervisor to restrict access to a case at their discretion. When a case is secured using this feature, it is only accessible to specifically designated employees. However, if a case is not secured, it remains viewable by any employee with RMS access. The Department generally defaults to keeping cases unsecured, as RMS is set up to facilitate collaboration among investigators and helps identify connections across various criminal investigations, including those spanning different bureaus, divisions, and investigative functions.

While not explicitly required by any written guidance, including the Detective Operations Manual, the Department informed the OIG that, in practice, numerous divisions and units already restrict access to sensitive cases. For example, access to homicide cases, counter-terrorism cases (Major Crimes Division), and criminal threat cases involving celebrities or City officials (Threat Management Unit) is limited to personnel assigned to those specific divisions or units. Department personnel outside of these divisions are unable to access related case information.[9]

Currently, investigators can manually restrict access to a case within RMS; however, this is not a default setting and must be applied to individual cases at the investigator's discretion. Additionally, there is an option to place a 'subscription' on a case file, notifying the lead investigator of any unauthorized attempts to access the information. The lead investigator can examine an Audit Log and Activity Log, which provide a comprehensive and detailed record of case access and activity. An added security feature of RMS is that only an RMS Administrator can delete records.

V. RESULTS AND FINDINGS

As a result of its review, the OIG found the following:

Finding 1. The OWB audit of 12 criminal sexual assault investigations conducted by the Department between 2017 and 2019, excluding the Moonves case, found no breaches involving the sharing of confidential information or evidence of interference by command staff. The OIG did not find any evidence to the contrary.

Finding 2. The OIG found that at the time of the Moonves case, the Department had policies, procedures, and controls in place regarding confidentiality and the disclosure of sensitive case information. These policies and procedures remain in effect today. However, the OIG has

[9] Certain types of investigations have significantly tighter access restrictions. For example, counter-terrorism investigations are maintained in a stand-alone database, further limiting who can view or be informed of these cases.

determined that the existing procedures and controls could be strengthened to better prevent inappropriate or unauthorized access and disclosure, both within the Department and externally.

Finding 3. The OIG found that the Department lacks clear guidance and standardized procedures on when and how to restrict access to case files and sensitive information. There is no established requirement specifying which cases must be restricted nor a defined process or criteria for making this determination.

Lastly, the OIG believes that even if more robust access restrictions and procedural controls had been in place during the Moonves criminal investigation, they likely would not have prevented the unauthorized sharing of confidential information between the detective, Palka, and Moonves. While strong procedural safeguards and access restrictions are essential for protecting sensitive information, they cannot always deter bad actors.

In this case, Palka—at the time he was the assistant commanding officer of OWB, which includes Hollywood Area—requested information from the detective, who ultimately shared it with him. Once in possession of that information, Palka was already prohibited by existing Department policies and state law from disclosing it to unauthorized individuals outside the Department, including Moonves, who was the subject of the criminal investigation. However, beyond Palka's own knowledge and adherence to these rules, the OIG does not believe that additional safeguards alone could have necessarily prevented the disclosure. The possibility of administrative or even criminal consequences was ultimately not enough to deter him.

VI. RECOMMENDATIONS

The OIG recommends the BOPC DIRECT the Chief of Police to do as follows:

Reaffirm the "Right-to-Know, Need-to-Know" Standard

1. Issue an order or directive reaffirming the "right-to-know, need-to-know" standard for data and information access and sharing.

Establish Standard Restrictions to Accessing Criminal Case Information

2. Establish clear, standardized procedures and criteria for determining which types of criminal cases require restricted access. These procedures should specify:

   a) The categories of cases that must be restricted;
   b) The personnel authorized to access restricted cases and the conditions under which access is permitted;
   c) The circumstances under which limited access may be granted to additional personnel; and,
   d) The requirements for maintaining restricted cases, including whether they should be housed in a separate stand-alone system.

VII. DEPARTMENT RESPONSE

The OIG submitted a draft of this report to the Department for its review. In response, the Department offered clarifications and proposed revisions regarding several issues. These suggestions were accepted by the OIG and integrated into the final report.

VIII. APPENDIX

The Department's complete response may be found attached.

APPENDIX: **LOS ANGELES POLICE DEPARTMENT'S RESPONSE TO THE OFFICE OF THE INSPECTOR GENERAL'S REVIEW OF THE LOS ANGELES POLICE DEPARTMENT'S CONTROLS OVER ACCESSING AND SHARING CONFIDENTIAL INFORMATION IN SEXUAL ASSAULT INVESTIGATIONS**

INTRADEPARTMENTAL CORRESPONDENCE

November 7, 2025
1.1

TO: Office of the Inspector General

FROM: Chief of Police

SUBJECT: LOS ANGELES POLICE DEPARTMENT'S RESPONSE TO THE OFFICE OF THE INSPECTOR GENERAL'S REVIEW OF THE LOS ANGELES POLICE DEPARTMENT'S CONTROLS OVER ACCESSING AND SHARING CONFIDENTIAL INFORMATION IN SEXUAL ASSAULT INVESTIGATIONS

The Los Angeles Police Department (Department) has received the Office of the Inspector General's (OIG) draft report of the Review of the Los Angeles Police Department's Controls Over Accessing and Sharing Confidential Information in Sexual Assault Investigations

The report includes two recommendations to be made as follows:

SECTION VI. RECOMMENDATIONS

1. Issue an order or directive reaffirming the "right-to-know, need-to-know" standard for data and information access and sharing; and,

2. Establish clear, standardized procedures and criteria for determining which types of criminal cases require restricted access. These procedures should specify: a) The categories of cases that must be restricted; b) The personnel authorized to access restricted cases and the conditions under which access is permitted; c) The circumstances under which limited access may be granted to additional personnel; and d) The requirements for maintaining restricted cases, including whether they should be housed in a separate stand-alone system.

Department Response

The Department concurs with the OIG's findings and the recommendations.

On November 6, 2025, the Department issued a Department-wide electronic directive reaffirming the "right-to-know, need-to-know" standard and further making clear that confidential information shall not be shared with a person who does not meet the same requirements.

Additionally, Detective Bureau is researching the feasibility of developing specific criteria for restricted case access. This evaluation will consider the technological abilities to use a stand-alone system, the potential operational impacts on the clearance rate for investigations done by geographic Areas, and any necessary additional internal controls to monitor cases with access granted to additional personnel.

Should you have any questions or concerns regarding this matter, please contact Deputy Chief Alan S. Hamilton, Chief of Detectives, Detective Bureau, at (213) 486-7000.

Respectfully,

JIM McDONNELL
Chief of Police