BUDGET & FINANCE

MOTION

GOVERNMENT OPERATIONS

On or around March 20, 2026, unauthorized access was reportedly discovered involving a third-party platform used to transmit and store discovery materials provided to opposing counsel and litigants. It is unclear when the City Attorney's Office became aware, what actions were taken, and when they were taken. City officials and employees were not formally notified of the breach and instead became aware of it largely through media reporting on April 7, 2026.

Preliminary information indicates that a substantial volume of records, including materials that may contain sensitive personnel data, was accessed and then circulated on social media platforms. The full scope of exposure, including the number of affected files and the extent of the dissemination, has not yet been verified. Questions remain regarding the third-party platform, including why it was used for sensitive materials, what security protections were in place, and whether appropriate access controls were implemented.

While the underlying criminal matters referenced in these materials may include closed cases, the public release of unredacted discovery files raises serious and ongoing concerns regarding the privacy and safety of City employees. It also raises potential risks to individuals who provided testimony or information under expectations of confidentiality. This could also compromise related or pending legal matters and undermine prosecutorial integrity.

This incident presents significant concerns for the City beyond any single department, including potential exposure to civil liability, risks to witness and employee safety, and broader questions regarding third-party vendor oversight and data storage practices across departments handling sensitive materials.

Given the seriousness of this breach, the City Council has a responsibility to ensure full transparency and accountability. This includes understanding not only what was accessed and exposed, but also how the breach occurred, how long the system was vulnerable, when the City Attorney's Office became aware, and why other City officials were not notified. It raises significant governance concerns that warrant immediate scrutiny, both to address the current breach and to strengthen safeguards against future exposure of sensitive City-held information.

I THEREFORE MOVE that the City Council REQUEST the City Attorney to appear before the City Council within 15 days to report on the following:

- A detailed accounting of the breach, including the total volume and categories of records accessed, exfiltrated, or exposed and types of sensitive information involved, including sensitive data contained in discovery materials;
- A clear timeline of events, including when the breach occurred, when it was first detected, when City departments and officials were notified, when and how the incident was

escalated internally, and when and how external notification or disclosure decisions were made; and

- An assessment of the City's potential legal exposure, including anticipated claims, litigation risks, or related proceedings arising from the data breach, a summary of applicable legal and regulatory notification requirements triggered by the incident, and steps taken to ensure compliance with all required notification obligations to impacted individuals, including: who has already been notified, who has not yet been notified, what criteria are being used to determine notification, and what protective measures are being offered.

I FURTHER MOVE that the City Council REQUEST the City Attorney to appear before the City Council in Closed Session within 15 days to present on the following:

- A detailed accounting of the breach, including categories of impacted individuals, including witnesses, City employees, and other third parties, the number of cases affected, and whether any matters remain under active litigation or related proceedings.

I FURTHER MOVE that the City Council INSTRUCT the Information Technology Agency (ITA), with the assistance of other relevant City departments, to report within 15 days with the following:

- Existing protocols for the storage, transmission, and access control of sensitive materials, the role and obligations of third-party vendors supporting these systems, identified vulnerabilities or failures that enabled unauthorized access, and a corrective action plan to remediate those vulnerabilities and strengthen safeguards;
- Technical details regarding how the system was accessed and how data was exfiltrated or exposed, categories and approximate volume of records impacted, and any known indicators of compromise or ongoing risk; and
- Steps taken to secure the third-party platform and prevent further access, measures implemented to strengthen security, and coordination with City departments to ensure protection of sensitive data moving forward.

PRESENTED BY _____
YSABEL JURADO
Councilmember, 14th District

APR 14 2026

SECONDED BY _____

ORIGINAL