



## CITY OF GLENDALE, CALIFORNIA REPORT TO THE CITY COUNCIL

### AGENDA ITEM

---

Report: Acceptance and appropriation of 2024 State and Local Cybersecurity Grant Program funds

1. Motion accepting \$250,000 in State and Local Cybersecurity Grant Program funds from the California Governor's Office of Emergency Services .
2. Resolution of Appropriation.

### COUNCIL ACTION

---

<b>Item Type:</b> Consent Calendar
<b>Approved for</b> <u>January 14, 2025</u> <b>calendar</b>

### EXECUTIVE SUMMARY

---

The California Governor's Office of Emergency Services (Cal OES) 2024 State and Local Cybersecurity Grant Program (SLCGP) provides \$250,000 for the City of Glendale to implement a Security Information & Event Management System (SIEM), review and develop Cybersecurity policies, and develop Disaster Recovery and Business Continuity plans; strengthening the City's cybersecurity posture.

## RECOMMENDATION

---

That the City Council approve the Motion accepting \$250,000 in 2024 SLCGP funds and adopt a Resolution of appropriation for those grant funds.

## ANALYSIS

---

On September 27, 2024, the City of Glendale submitted a grant application to Cal OES requesting \$250,000 in funding. Cal OES awards grants to eligible local agencies and tribal governments through a detailed review process. The maximum grant award per entity is \$250,000.

The Information Technology Department staff conducted an internal cybersecurity assessment. The assessment identified opportunities to enhance our cybersecurity posture in the areas of threat governance, detection, response, and recovery capabilities.

With the information gathered from that cybersecurity assessment, the grant funding will enable the City to directly support the City's efforts in enhancing its cybersecurity capabilities in the following areas:

- **Acquire and implement a Security Information and Event Management (SIEM) system.** This will enhance in advanced threat detection, incident response, and security monitoring capabilities.
- **Engage a consulting firm to review and update existing Cybersecurity policies.** This will ensure alignment of the City's internal policies with current best practices and regulatory requirements (e.g. Criminal Justice Information Systems (CJIS), and Payment Card Industry Data Security Standard (PCI).
- **Develop and implement comprehensive Disaster Recovery and Business Continuity plans.** These plans will outline procedures for responding to and recovering from cyber incidents, minimizing disruption to city services, and ensuring compliance with relevant regulations.

The implementation of these efforts will also ensure compliance with various regulatory requirements, including those related to Criminal Justice Information Services (CJIS), Payment Card Industry Data Security Standard (PCI DSS), and the NIST Cybersecurity Framework adopted by the City. The SIEM system will play a crucial role in meeting the legal and regulatory requirements for security event logging and audit record retention.

## STAKEHOLDERS/OUTREACH

---

N/A

## FISCAL IMPACT

---

As the State and Local Cybersecurity Grant Program award was not incorporated into the approved FY 2024-2025 budget, therefore the Information Technology Department respectfully requests an appropriation of \$250,000 from State Grant Revenue. The appropriation request is outlined below:

Requesting Appropriation			
Amount	From (Account String)	To (Account String)	Funding Source
\$250,000	32610-6030-ISD-0020-P0000 ISD01330AG	43110-6030-ISD-0020-P0000 ISD01330AG	ITD Infrastructure Fund – State Grant

## **ENVIRONMENTAL REVIEW (CEQA/NEPA)**

N/A

## **CAMPAIGN DISCLOSURE**

This item is exempt from campaign disclosure requirements.

## **ALTERNATIVES TO STAFF RECOMMENDATION**

**Alternative 1:** In the event that council denies the Information Technology's request to accept and appropriate the grant funds, the City funding would be needed to procure a Security Information & Event Management System (SIEM), develop Cybersecurity policies and Disaster Recovery and Business Continuity plans.

**Alternative 2:** The City Council may consider alternative approaches not outlined by staff.

## **ADMINISTRATIVE ACTION**

**Submitted by:**

Jason Bradford, Chief Information Officer

**Prepared by:**

Chris Lemus, Cybersecurity Manager

Jason Miller, Assistant Chief Information Officer

**Approved by:**

Roubik R. Golanian, P.E., City Manager

## **EXHIBITS/ATTACHMENTS**