ARAPAHOE COUNTY

Arapahoe County

5334 South Prince Street
Littleton, CO 80120
303-795-4630
Relay Colorado 711

Board Summary Report

File #: 24-366 **Agenda Date:** 7/1/2024 **Agenda #:**

To: Board of County Commissioners

Through: Philip Savino, Director, Information Technology

Prepared By:
Philip Savino, Director, Information Technology

Presenter: Philip Savino, Director, Information Technology

Subject:
2:00 PM *State and Local Cybersecurity Grant Program CrowdStrike Grant

Purpose and Request:
The purpose of this report is to discuss the State and Local Cybersecurity Grant Program for CrowdStrike Falcon Complete, a Managed Detection and Response (MDR) System to detect and mitigate cybersecurity threats.

Background and Discussion:
The Information Technology Department wishes to seek approval to apply for the State and Local Cybersecurity Grant Program (SLCGP), a federal initiative aimed at enhancing the cybersecurity posture of state, local, tribal, and territorial (SLTT) governments across the United States. The grant would supply Arapahoe County with 2,768 CrowdStrike agents for ACG workstations and 354 CrowdStrike agents for ACG Servers.

Established under the Infrastructure Investment and Jobs Act, the program is designed to provide financial assistance to these entities to develop and implement comprehensive cybersecurity plans, improve their capabilities to detect and respond to cyber threats, and reduce the risks of cyber incidents.

The SLCGP provides funding for cybersecurity initiatives including:

- Enhancing the security of critical infrastructure.
- Deploying advanced cybersecurity technologies.
- Developing and updating cybersecurity plans.

The program is funded from the Federal Emergency Management Agency (FEMA FY23 SLCGP). SLCGP requires that participants move to adopt Cybersecurity Best Practices. The Colorado Office of Information Technology (OIT) acts as a purchasing agent to optimize pricing, offering endpoint encryption to the participating local governments. Local governments will be able to continue with the purchased endpoint encryption in future years with their own funding.
CrowdStrike Falcon Complete is a managed endpoint detection and response (MDR) system provided by CrowdStrike, a leading cybersecurity company. Falcon Complete offers a comprehensive suite of cybersecurity

services, including real-time threat detection, incident response, and threat intelligence. Key features of CrowdStrike Falcon Complete include:

- **Real-Time Threat Detection:** uses machine learning and behavioral analytics to identify and block threats in real-time.
- **24/7 Monitoring:** Provides around the-clock monitoring by a team of cybersecurity experts. (*A feature that Microsoft Defender 365 does not offer with their unpaid version*.)
- **Incident Response**: Offers rapid response to security incidents to mitigate damage and restore operations with a $1 Million dollar guarantee. (*A feature that Microsoft Defender 365 does not offer with their unpaid version*.)
- **Threat Intelligence:** Delivers actionable intelligence on emerging threats and vulnerabilities. (*A feature that Microsoft Defender 365 does not offer with their unpaid version.*)
- **Automated Remediation:** Automatically isolates and removes threats from endpoints.

Match Not Required for FY2023
The Governor's Office of Economic Recovery has provided a grant to cover the required 20 percent match for local governments. The funding source is Infrastructure Investment and Jobs Act Cash Fund (IIJA), SB 22-0215. Applicants will not be required to provide a 20 percent in-kind or cash match for this round of funding.

Members of the Cybersecurity Subcommittee (CAC) of Homeland Security and All-Hazards Senior Advisory Committee (HSAC) serve as the steering committee for this grant. The CAC meets first Wednesday of each month from 10-11 a.m. The HSAC Cyber group will be discussing if Year 3 SLCGP funds should look different from what was done in years 1 and 2.

FEMA has indicated that the intent to have the match increase future funding.

- Federal Fiscal Grant Year 2024: 30% projected match
- Federal Fiscal Grant Year 2025: 40% projected match

Due Dates:

- Application Submission Deadline: Tuesday, July 9, 2024
- Notification of Award Recommendation: Friday, July 26, 2024
- Request for Reconsideration: Friday, August 2, 2024

Fiscal Impact: None

Alternatives: The current state would be to remain without a Managed Detection and Response system, increasing the risks of cybersecurity threats to Arapahoe County's workstations, servers, and ultimately overall services.

Alignment with Strategic Plan:

☒Be fiscally sustainable.
☒Provide essential and mandated service.
☒Be community-focused

Staff Recommendation: The Information Technology Department recommends that the Board of County Commissioners support applying for the SLCGP grant to fund CrowdStrike Falcon Complete.

Concurrence: None