BOARD OF SUPERVISORS
AGENDA LETTER

Clerk of the Board of Supervisors
105 E. Anapamu Street, Suite 407
Santa Barbara, CA 93101
(805) 568-2240

Agenda Number:

Department Name:	Information Technology
Department No.:	067
For Agenda Of:	June 25, 2024
Placement:	Administrative
Estimated Time:	
Continued Item:	No
If Yes, date from:	
Vote Required:	Majority

TO: Board of Supervisors

FROM: Department Director(s): Chris Chirgwin, CIO (805) 568-2608
Contact Info: Andre Monostori, Deputy CIO (805) 568-2606

SUBJECT: **Agreement for Professional Services of Independent Contractor with Red Canary, Inc., for Cybersecurity End-Point Protection Services, All Districts.**

County Counsel Concurrence
As to form: Yes

Other Concurrence: Select_Other
As to form: Yes

Auditor-Controller Concurrence
As to form: Yes

Recommended Actions:

That the Board of Supervisors:

a) Approve and authorize the Chair to execute the Agreement with Red Canary to procure continued cybersecurity protection services for up to 5,900 County computers and 4,700 users for monitoring, in the amount not to exceed $319,000 for Fiscal Year 2024-25; and

b) Approve and authorize the Chief Information Officer or their designee to order additional services in an amount not to exceed 5% of the contract amount, or $15,950; and

c) Determine that the above recommended actions are government funding mechanisms or other government fiscal activities, which do not involve any commitment to any specific project that may result in a potentially significant physical impact on the environment and is therefore not a project under the California Environmental Quality Act (CEQA) pursuant to section 15378(b)(4) of the CEQA Guidelines.

Summary:

This item is before the Board to approve the agreement for cybersecurity end-point protection services with Red Canary, for Fiscal Year 2024-25 in an amount not to exceed $319,000 (Attachment A).

Background:

The Information Technology Department (ITD) is currently engaged with two Managed Security Services Providers (MSSPs), Critical Start and Red Canary for Security Operations Center (SOC) services for workstation and servers respectively. Critical Start has recently informed us that we need to secure Microsoft Sentinel to complete our server migration to their SOC services, at an additional cost of $300,000 (to Microsoft). This unexpected expense prompted us to explore other vendor/options for this service. Having confirmed with our other SOC service provider, Red Canary, that they do not have this requirement and associated expense, we propose moving all SOC services to Red Canary beginning July 2024. Red Canary is a leading MSSP providing 7x24/365 security monitoring and response services.

Leveraging economies of scale, this change will save money by using only one vendor for these services. Contracting with a single MSSP brings vulnerability management to a single pane of glass, enhancing visibility into our cybersecurity posture and increasing operational efficiencies.

The County has been a customer of Red Canary since 2018. In 2023 we moved a portion of our endpoint protection services to M365. Red Canary was not in a position to support the Government Community Cloud (GCC) at that time. The County engaged Critical Start to fill this need. Red Canary can now support GCC-based customers, which will allow us to move back to a unified service.

We have opted out of the current Critical Start contract by giving them 30 days' notice on May 30, 2024 in alignment with our agreement.

Performance Measure:

Red Canary key abilities include specialized dashboards and reporting to pre-designated contacts. These dashboards and reports shall include:

- Situation Awareness and urgent actions
- Recent Activity for security alert, investigation, and response metrics
- Measurement and performance management improvements for COUNTY's security analysts
- Performance indicators for Red Canary SOC efficiency and metrics
- Key performance indicators for technology effectiveness of the Supported Product(s)
- Threat Content Detection and Open/Closed alerts mapped to MITRE ATT&CK Matrix framework

Performance Metrics for Red Canary's service over the most recent 6 months show the service performs well:

- Coverage: 0 false negatives where Red Canary failed to identify threatening behavior.
- Accuracy: 100% of the 40 threats detected by Red Canary were true positives.
- Timeliness: 62% of the 35 medium and high severity threats were identified in less than 2 hours.

Contract Renewals and Performance Outcomes:

Red Canary will meet all Service Level Agreements (SLAs) agreed to by ensuring security events are responded to by the vendor within the defined timeframes per the SLAs. Event responses that fail to meet the SLAs will be credited back to the County.

Fiscal and Facilities Impacts:

Budgeted: Yes

Fiscal Analysis:

Funding Sources		Total FY 24-25 Cost
ITD Internal Service Fund 1915		
Annual Renewal	$	319,000.00
5% contingency	$	15,950.00
Total	$	334,950.00

Narrative: Funding to cover the cost is included in the IT Shared Services Internal Service Fund (ISF) rates FY 2024-25 Information Technology Fund 1915 budget, including funding to cover the 5% contingency amount of $15,950.

Special Instructions:

Clerk of the Board: Please return one (1) duplicate of the executed agreement plus the minute order of the action to the Information Technology Department, attention: Onelia Rodriguez, Finance Manager.

Attachments:

1. Attachment A—Red Canary Agreement

Authored by:

Jason Womack, Department Business Specialist, Information Technology Department