



# San Bernardino County Employees' Retirement Assoc.

## Staff Report Details (With Text)

<b>File #:</b>	19-568.1	<b>Name:</b>	
<b>Type:</b>	Consent Item		
<b>File created:</b>	10/18/2019	<b>In control:</b>	BOARD OF RETIREMENT
<b>On agenda:</b>	11/7/2019	<b>Final action:</b>	
<b>Title:</b>	Approve a proposed contract with Secureworks in the sum of \$38,988 (plus applicable sales taxes) to provide cybersecurity detection and prevention and endpoint threat monitoring.		
<b>Sponsors:</b>			
<b>Indexes:</b>			
<b>Code sections:</b>			
<b>Attachments:</b>	1. Exhibit A: Secureworks Proposal, 2. Exhibit B: Cybersecurity Managed Services Recommendation		

Date	Ver.	Action By	Action	Result
------	------	-----------	--------	--------

**FROM:** Joe Michael, Chief Information Officer

**SUBJECT:** Cybersecurity Monitoring Services

### RECOMMENDATION:

Approve a proposed contract with Secureworks in the sum of \$38,988 (plus applicable sales taxes) to provide cybersecurity detection and prevention and endpoint threat monitoring.

### BACKGROUND:

SBCERA is requesting to engage Secureworks to provide cybersecurity detection and prevention, along with endpoint threat monitoring. By contracting for these services, SBCERA can leverage Securework's detection algorithms which analyze and compare data from over 310 billion cyber-events daily, ensuring data coming into and out of our networks is being monitored for the latest threats. In addition, the services provides 24-hour, 365-day monitoring, allowing SBCERA information technology staff to focus on critical real time events as opposed to lower value monitoring and review of endless streams of data on a manual basis.

Staff reviewed the leading cybersecurity monitoring firms identified in the 2019 Gartner Group and 2018 Forrester Managed Security Services Provider (MSSP) reports. After reviewing managed cybersecurity monitoring approaches from other "magic quadrant" leaders, staff believes that the approach provided by Secureworks is the most robust solution and provides the fastest response time (within 15 minutes) of notification. It also allows for a tiered approach to detection based on perceived threat and time of day. Secureworks' solution combines both an on-premises solution which gathers data real-time as well as a cloud solution that analyzes that data against known threats. In addition, it includes data points from the desktops giving us a complete picture of traffic patterns. The solution provides the opportunity for us to add on (at an additional cost in the future) best practice response policy and procedure creation tailored to our environment, as well as access to a breach event response team. The team would be available to come physically on site to help

contain a breach should one occur, ensure the correct data elements are retained for law enforcement, and assist with data recovery to bring the networks back to a fully functional state.

The Secureworks proposal is attached as Exhibit A. Attached as Exhibit B is a staff memorandum memorializing additional information on the Gartner/Forrester reports.

**BUDGET IMPACT:**

Costs for this item are included in the current year administrative budget.

**STRATEGIC PLANNING GOAL/OBJECTIVE:**

Operational Excellence & Efficiency

**COMMITTEE REVIEW:**

This item was reviewed by the Administrative Committee at its October 17, 2019 meeting and recommends Board approval, with a 3-0 vote. Trustee Bracco was absent from the meeting.

**STAFF CONTACT:**

Joe Michael

**ATTACHMENTS:**

Exhibit A: Secureworks Proposal

Exhibit B: Cybersecurity Managed Services Recommendation