Office of the City Manager

CONSENT CALENDAR
December 14, 2021

To: Honorable Mayor and Members of the City Council

From: Dee Williams-Ridley, City Manager

Submitted by: LaTanya Bellow, Interim Deputy City Manager

Subject: Contract 32100185 Amendment: Digital Hands for Endpoint Detection and Response (EDR) Monitoring

RECOMMENDATION

Adopt a Resolution authorizing the City Manager to amend contract number 32100185 with Digital Hands, for Cybersecurity Event Monitoring and Security Information and Event Management (SIEM), increasing the previously authorized contract amount by $381,137, for a total not to exceed amount of $ $996,117.00 from December 15, 2021 to June 30, 2024.

FISCAL IMPACTS OF RECOMMENDATION

Funding for these professional services is available in the Department of Information Technology's Fiscal Year (FY) 2022-2024 IT Cost Allocation Fund as outlined below. Spending for this contract in future fiscal years is subject to Council approval of the proposed citywide budget and annual appropriation ordinances.

202,991	FY 2022: Professional Services
	Budget Code: 680-35-363-382-0000-000-472-613130-
	(IT Cost Allocation, Security, Professional Services)
$202,991	**Sub-Total: FY 2022 Professional Services**
96,496	FY 2023: Professional Services
	Budget Code: 680-35-363-382-0000-000-472-613130-
	(IT Cost Allocation, Security, Professional Services)
$ 96,496	**Sub-Total: FY 2023 Professional Services**
81,650	FY 2024: Professional Services
	Budget Code: 680-35-363-382-0000-000-472-613130-
	(IT Cost Allocation, Security, Professional Services)

$ 81,650	**Sub-Total: FY 2024 Professional Services**
$381,137.00	**Total: FY 2022-2024 Professional Services**

CURRENT SITUATION AND ITS EFFECTS

The City of Berkeley (The City) previously authorized, under resolution no. 69,521-N.S., the City Manager to enter into a contract with Digital Hands, for Cybersecurity Event Monitoring and Security Information and Event Management (SIEM). The contract was executed on June 11, 2021. And, onboarding of Digital Hands managed security services provider basic monitoring (MSSP) began June 4, 2021.

Due to limitations in funding, that resolution only included spending authority to cover the one-time onboarding fee for the City's "End Point Protection and Detection/ Response (EPP/EDR/MDR)" and only one of three years' worth of the annual fee to cover the ongoing monitoring. This resolution adds the additional two years' worth of annual fees for End Point Protection and Detection/ Response (EPP/EDR/MDR) threat hunting and distributes them over the life of the contract.

Secondly, during contract negotiations and onboarding of Digital Hands, the City also added new cybersecurity sensors to its portfolio. This resolution adds the annual fees for these sensors and distributes them over the life of the contract.

Finally, with the expansion of and change out of data sources (such as, servers and databases) within the City already completed since last December as well as planned over the life of this contract, this resolution adds the annual fees for these computing sources and distributes them over the life of the contract.

BACKGROUND

In 2018, the City developed a Cyber Resilience Plan (CRP) to provide the City a situational awareness of our cyber-risk exposure, the maturity of its cyber-security capabilities, the City's efficiency in addressing regulatory compliance, and to provide action items that ensure the City is equipped to handle cyber-attacks and mitigate the effects of a successful cyber-attack.

The CRP divided this effort into two sets of work: an as-is assessment and a to-be roadmap. In February 2020, the City of Berkeley issued a Request for Proposal (RFP) No. 20-11385-C for addressing two highest priority action items from the CRP:

Part A: Managed Security Service Provider (MSSP/SIEM)
Part B: End Point Protection and Detection/Response (EPP/EDR/MDR) / Threat Hunting

On June 11, 2021, the City entered into a contract with Digital Hands that (i) provides for Part A, (ii) allows the City to add Part B when the spending authority becomes adjusted to cover all three years of the annual fee, and (iii) allows the City to adjust the cost when and as the City further authorizes (a) changes in the number of systems being monitored – such as increases or decreases in the total number of servers and databases – (b) changes in the services or scope of services – such as new monitoring capabilities like EPP/EDR/MDR – and (c) changes in the cybersecurity sensors – such as those added by December 2020's AA01.

With the changes experienced in 2020 and thus far in 2021 in the cyber-threat and cyber-insurance marketplace, active monitoring – as opposed to alert-driven response – that includes both Part A (MSSP/SIEM) and Part B (EPP/EDR/MDR) has become the minimum expectation. The City thus needs to expeditiously move our EPP/EDR/MDR monitoring and its associated threat hunting service to Digital Hands as was intended under part of AAO1 in December 2020. Fiscal Year 2022 budget rectifies the funding gap.

December 2020 AAO1 also added new cybersecurity sensors to the City's portfolio that need to be picked up in accordance with the contract. Most of these sensors pertain to Part A services. And finally, the number of systems being monitored has increased within the past year. These new servers and databases, as well as those planned for and being added in FY22 also need to be covered by Part A and Part B in accordance with the contract.

Lastly, the CRP aligns with the City's adopted Strategic Plan goals of:

- Create a resilient, safe, connected, and prepared City
- Provide state-of-the-art, well-maintained infrastructure, amenities, and facilities
- Be a customer-focused organization that provides excellent, timely, easily-accessible service and information to the community; and adopts the strategies which align with the five (5) year Digital Strategic Plan (DSP).

ENVIRONMENTAL SUSTAINABILITY AND CLIMATE IMPACTS

All event monitoring and SIEM services – both Part A and Part B – are conducted remotely thus eliminating the need for travel to Berkeley, resulting in a reduction of greenhouse gas emissions for travel.

RATIONALE FOR RECOMMENDATION

This increase in spending authority satisfies the updated cyber-insurance minimum expectation of the changing cyber-treat environment while it also fulfills the scope of the RFP No. 20-11385-C over the life of the entire contract with Digital Hands. It also co-terms Part B (EPP/EDR/MDR) active monitoring and distributes the costs over the life of the contract. And, it makes changes in the number of systems being monitored as well as in the type of cybersecurity sensors, in accordance with the contract.

ALTERNATIVE ACTIONS CONSIDERED

The City considered hiring additional staff to increase coverage for active monitoring of EPP/EDR/MDR to 24/7/365. This option is cost prohibitive and not sustainable because incident response analysts, and especially those that specialize in this type of tool, are among the highest paid and most high turnover positions in cybersecurity.

The City also considered alert-driven monitoring of the EPP/EDR/MDR and of the AAO1 added cybersecurity sensors. However, that would leave the City vulnerable to advanced attacks (such as ransomware) during off hours and non-workdays, could put our existing cyber-insurance in jeopardy, and would reduce the City's ability to obtain cyber-insurance next year.

CONTACT PERSON
LaTanya Bellow, Interim Deputy City Manager, (510) 981-7000

Attachments:
1: Resolution

RESOLUTION NO. ##,###-N.S.

CONTRACT 32100185 AMENDMENT: DIGITAL HANDS FOR ENDPOINT DETECTION AND RESPONSE (EDR) MONITORING

WHEREAS, the City has entered into a contract with Digital Hands to provide 24/7/365 active monitoring for cybersecurity events; and

WHEREAS, said contract anticipates and is flexible enough to accommodate changes in the number of systems being monitored; and

WHEREAS, said contract anticipates and is flexible enough to add 24/7/365 active monitoring of the City's growing set of cybersecurity sensors; and

WHEREAS, said contract anticipates and is flexible enough to add 24/7/365 active monitoring (also called "threat hunting") of the City's EPP/EDR/MDR; and

WHEREAS, Funding for these services is available in the Department of Information Technology's IT Cost Allocation Fund, and spending for this contract in future fiscal years is subject to Council approval of the proposed citywide budget and annual appropriation ordinances.

NOW THEREFORE, BE IT RESOLVED by the Council of the City of Berkeley that the City Manager is authorized to amend contract number 32100185 with Digital Hands, for Cybersecurity Event Monitoring and Security Information and Event Management (SIEM), increasing the previously authorized contract amount by $381,137, for a total not to exceed amount of $ $996,117.00 from December 15, 2021 to June 30, 2024.