KROLL

STATEMENT OF WORK
FOR
Kroll Responder powered by Red Canary

This Statement of Work ("SOW"), dated July 13, 2023, is entered into pursuant to and incorporates herein by reference the letter of engagement, entered into as of February 8, 2019 (together with this SOW, the "Agreement"), by and between County of Santa Barbara ("Client") and Kroll Associates, Inc. on behalf of itself and its affiliates ("Kroll") for the Kroll Services described herein. Capitalized terms herein shall have the meaning ascribed in the letter of engagement.

Kroll Services and Red Canary Services are described below and subject to the respective terms and conditions referenced herein.

A. **Kroll Endpoint Response and Remediation Support Services ("Kroll Services")**

As part of **Kroll Responder powered by Red Canary** service, Kroll will provide the following Kroll Services to Client:

Description of Kroll Services
24x7 Endpoint Response and Remediation Support Kroll will provide managed remote endpoint response and remediation support for medium and high severity Threat Alerts issued by Red Canary, 24x7x365. Kroll's incident analysts will review issued Threat Alerts, and using the Client Portal and Endpoint Collection Software, will remotely triage, investigate, and respond to these alerts in an effort to effectively contain and/or remediate the identified threat on actively monitored and online Endpoints. Kroll will provide Client with follow-up update(s) and guidance regarding remediation steps taken, along with required Client follow-up actions and Kroll recommendations. Kroll's responsive actions may be limited or modified through written rules of engagement and response playbooks (including the configuration of Red Canary Automate orchestration features) as mutually agreed between Client and Kroll during the Term. In addition, Kroll will provide the following throughout the Term: • Periodic threat landscape, detection review, and service update teleconferences • Threat analysis and intelligence advice for new or emerging threats of interest • Threat Alert correlation and root cause analysis • Malware analysis and remediation guidance • E-mail based customer support for non-emergency requests, 09:00 to 17:00 EST/EDT, Monday through Friday– excluding U.S. Federal holidays. Client understands and accepts that, while not anticipated, any response and remediation actions taken could cause unforeseen system errors, outages, or data loss. **On-Demand Cyber Security Services**

As an active Kroll Responder Client, Kroll may be engaged to provide additional advisory, incident response and investigative services at a 15% discount from Kroll's standard rates, including:

- On-site and remote incident response services
- On-site and in-lab forensic imaging and analysis
- Custom digital forensic investigations
- Proactive advisory and assessment services

On-Demand Cyber Security Services are available upon request and subject to the execution of a separate Statement of Work between Kroll and Client.

B. Fee Structure and Invoicing

The initial term of this Statement of Work shall be for six (6) months ("Initial Term") from the date above ("Effective Date") and may be renewed for successive six-month periods upon mutual written agreement between the parties (each a "Renewal Term"), unless either Party provides written notice of termination to the other Party. Upon receipt of written notice, the effective date of the Termination shall be the end of the then-current Initial Term or Renewal Term. From the Effective Date, the Initial Term and any Renewal Term(s) together until termination hereunder shall be the "Term".

Invoicing for Managed Threat Detection Services. On behalf of its strategic partner, Red Canary, Kroll shall invoice Client for the Kroll Services and the Red Canary Services on a fixed fee basis for 5,800 Endpoints ("End User's Endpoints"). The fee for the Initial Term is $228,015.00. "Endpoint" means any kind of computing device that the Endpoint Collection software supports.

Kroll shall invoice the Client in full for the annual cost of this service in advance of the Effective Date of the Initial Term, and no more than to forty-five (45) days prior to the start of any Renewal Term. **The Term is not cancellable, and all payments are non-refundable.** Payment is due upon receipt of the invoice and all payments are required in US Dollars (USD).

Endpoint Overages. During any calendar month of the Term, in the event that the number of monitored Endpoints exceeds the number of End User's Endpoints listed above ("Overage"), Client will be invoiced for the Overage during the calendar quarter immediately following the onset of the Overage at a price that is pro-rated based on the cost listed above and the date of increase, and each quarter thereafter in which the monthly quantity of Endpoints monitored exceeds this amount.

Invoicing for On-Demand Cyber Security Services.
In accordance with the description of Kroll Services above, during the Term, Kroll may provide On-Demand Cyber Security Services to Client, subject to execution of an additional Statement of Work. The Professional Fees for this service will be charged at Kroll's then-current hourly rates, less a discount of 15%.

Kroll's current hourly rates are as follows:

Consulting Services	US$550/hour
Travel Time	50% of Consultant hourly rate
Media Preservation/Replication	US$400/media
Media / Data Storage	US$25/media/month

For On-Demand Cyber Security Services, Kroll shall invoice Client for the services performed on a monthly basis with the fee due and payable within thirty (30) days of the date of the invoice. In addition to the Professional Fees identified above, additional charges may include travel time, travel costs, and reasonable out-of-pocket expenses incurred in connection with these services.

To the extent Kroll is requested to provide any written testimony or reports, such additional services will be provided at Kroll's standard applicable hourly rates. However, oral testimony at deposition, a hearing or trial will be provided at 1.5 times such rates.

Accepted and agreed:

[CONTINUE TO NEXT PAGE]

C. **Red Canary Managed Threat Detection Services ("Red Canary Services")**

As Kroll's strategic partner in providing the **Kroll Responder powered by Red Canary** service, Red Canary will be responsible for providing the following Red Canary Services to Client, subject to Client's acceptance of, and provided pursuant to, the Red Canary Terms and Conditions ("EUSPA"), which terms and conditions are accessible via the applicable link below.

Additionally, Client further accepts and agrees to the terms of the Software End User License Agreement(s) ("VMware EULA") for the Endpoint Collection Software, which is defined and accessible via the link(s) listed in the table below.

In connection with the Kroll Responder powered by Red Canary services, Client acknowledges and agrees that Client's acceptance of and agreement to the Red Canary Terms and Conditions and the VMware EULA as evidenced by Client's signature below, is required for the provision of the Red Canary Services by Red Canary.

Description of Red Canary Services
Third Party Services: Red Canary Managed Threat Detection Services, provided by Red Canary for use by Client and Kroll pursuant to the Red Canary Terms and Conditions at https://redcanary.com/wp-content/uploads/2020/11/Red-Canary-Terms-and-Conditions-v2020-1-K.pdf. • Includes 24x7x365 Red Canary Threat Alert escalation and Portal access. • Includes Automate features
Threat Alerts: Red Canary will provide, as appropriate, Threat Alerts. "Threat Alerts" means analyst-vetted alerts on malicious activity detected by Red Canary on Client Endpoints. Threat Alerts will be sent to Kroll and Client's technical contacts as configured in the Red Canary Portal. Where applicable, each Threat Alert includes information describing the background of the threat related to the particular Alert. Threat Alerts will contain information that is known to Red Canary about the threat at the time, which typically includes but is not limited to: • Summary of the detected threat • Name of affected endpoint and user • Artifacts such as file names, Internet Protocol (IP) addresses, domain names and registry keys that help support both Client remediation efforts and identification of similar threats.
Client Portal: Client and Kroll will be provided with access to the Red Canary portal ("Portal") through which Client and Kroll can view data and Threat Alerts.

Client's Software License ("WMware EULA")
Third Party Software: The Red Canary Services include the provision of endpoint monitoring using VMware Carbon Black EDR software ("Endpoint Collection Software"), which is provided to Client in connection with the Red Canary Services and licensed hereunder for use by Red Canary on behalf of Client per the terms and conditions of the VMware EULA accessible at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/universal_eula.pdf

D. **Client Responsibilities**

In connection with the Kroll Services and Red Canary Services, Client agrees to be responsible for performing the following tasks:

1. Installing and maintaining active Endpoint Collection Software on all Client systems to be monitored.
2. Provide Kroll and Red Canary with continuous access to Client's instance of the Endpoint Collection Software to facilitate ongoing monitoring and response activities for the monitored Endpoints.
3. Obtaining all required authorizations to perform the Managed Threat Detection Services and any data or information required thereby. Client shall obtain consents and authorizes for Kroll and Red Canary and their employees and agents to gain access to and retrieve Technical Data and analyze Threat Alerts and to perform the Red Canary Services and the Kroll Services.
4. In the course of accessing, obtaining and otherwise using the Managed Threat Detection Services and Threat Alerts, Client shall have sole responsibility for the accuracy, quality, integrity, and authorization for use, and intellectual property ownership or right to use necessary for the transferability to Red Canary and Kroll of Technical Data.
5. Client will permit Kroll to include anonymized data that Kroll obtains from the monitoring of Client's endpoints in Kroll's proprietary threat intelligence database or feeds, as well as sharing any such data with its intelligence partners. This data includes binary hashes, binary metadata, and EDR event data such as process hashes, IP addresses, domain names, user context (System vs. Local, Root, Network Service, etc.) and operating system version identifiers.

Client's signature below hereby accepts and agrees to the description of Services and Client Responsibilities above and to the terms and conditions accessible in the links below for the Red Canary Services and Endpoint Collection Software:

1. the EUSPA: https://redcanary.com/wp-content/uploads/2020/11/Red-Canary-Terms-and-Conditions-v2020-1-K.pdf and
2. the VMware EULA: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/universal_eula.pdf

KROLL

Billing Information Form

Please complete the following information and return for Kroll's engagement. Insurance information only needed for events being submitted under a claim.

Client Contact

Primary Contact: Name/Title	Andre Monostori, Deputy Chief Information Officer
Telephone	
Email Address	amonostori@countyofsb.org
Additional Contact: Name/Title	Onelia Rodriguez, Finance Manager
Telephone	
Email Address	itdfinance@countyofsb.org

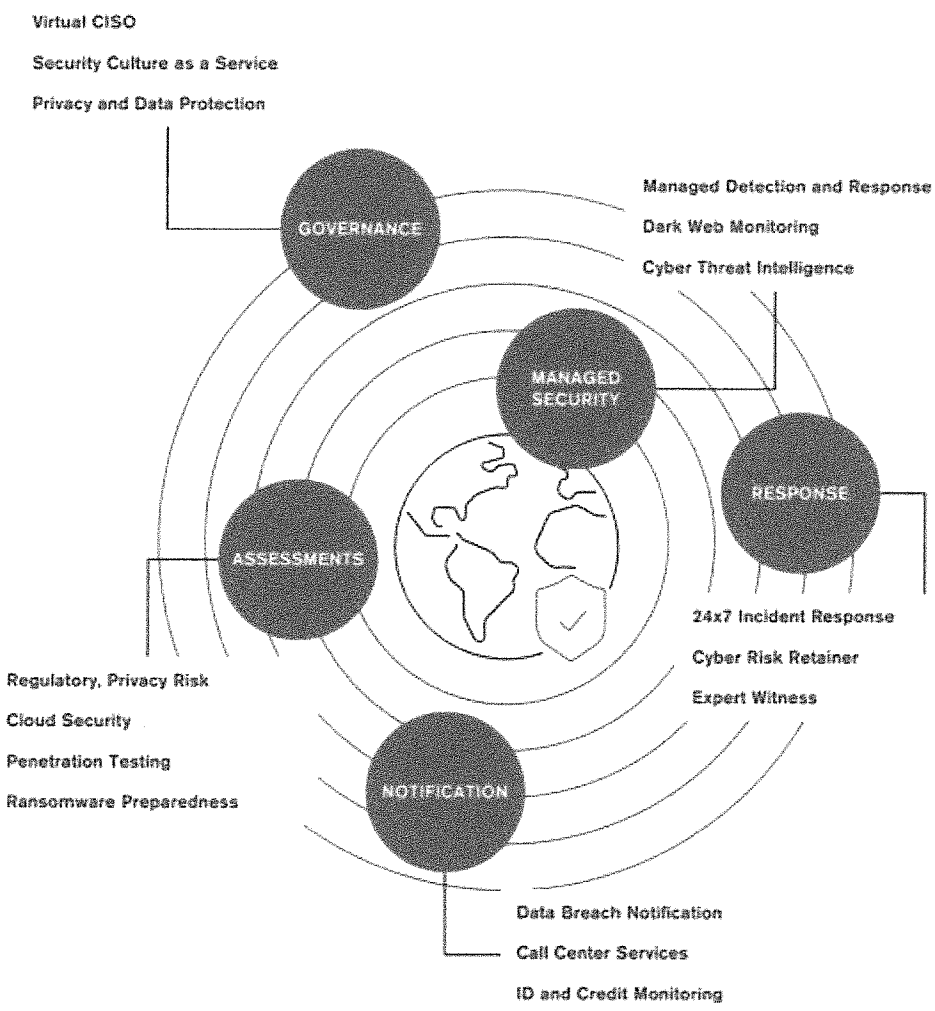
Billing Information

Address bill to	105 E. Anapamu Street, Room 304, Santa Barbara, CA 93101
Billing Physical Address	105 E. Anapamu Street, Room 304, Santa Barbara, CA 93101
Billing Email Address	itdfinance@countyofsb.org
Purchase Order #	

Insurance Information (if applicable)

Carrier (Insurer)	
Claim #	
Claims Handler Name/Title	
Telephone	
Email Address	
Insurance Broker Name/Title	
Telephone	
Email Address	

GLOBAL, END-TO-END CYBER RISK SERVICES



Additional Governance Risk Advisory Services

- Business Intelligence and Investigations
- Compliance Risk and Diligence
- Expert Services
- Financial Services Compliance and Regulation
- Information Management and Governance
- Security Risk Management

IN WITNESS WHEREOF, the Parties have executed this Agreement to be effective on the date executed by COUNTY ("Effective Date").

ATTEST:

Mona Miyasato
County Executive Officer
Clerk of the Board

By: Shiloh de la Guerra
Deputy Clerk

COUNTY OF SANTA BARBARA:

By: _____
Chair, Board of Supervisors

Date: 7-11-23

RECOMMENDED FOR APPROVAL:

Information Technology Department

By: DocuSigned by: Chris Chirgwin
D97209A7A68A4A0...
Chris Chirgwin, CIO

CONTRACTOR:

Kroll Associates, Inc.

By: _____
Authorized Representative

Name: Marc Brawner

Title: Managing Director

APPROVED AS TO FORM:

Rachel Van Mullem
County Counsel

By: DocuSigned by: Lauren Wideman
8F464D822C84458...
Deputy County Counsel

APPROVED AS TO ACCOUNTING FORM:

Betsy M. Schaffer, CPA
Auditor-Controller

By: DocuSigned by: Robert Geis IV
02B49B53797F440...
Deputy

APPROVED AS TO FORM:

Risk Management

By: DocuSigned by: Greg Milligan
DC240AC1E64247D...
Risk Management