EXHIBIT B

SOLE SOURCE/SOLE BRAND JUSTIFICATION

OVERVIEW:

Contracts/Purchasing recognizes that departments often invest a great deal of time and effort in selecting a source or brand, prior to submitting a requisition to Purchasing. Even though the department's review process prior to the submittal of a requisition may be sound, departments may unknowingly discourage free and open competition by requesting a single vendor or product. Additionally, the County is bound by both federal and local laws as well as County Policies of which County Staff may be not be aware of. The lack of an effective means of communication between buyer and requesting departments can lead to both lost time in completing the requisition as well as possible adverse legal actions towards both the County and the requesting staff member. Purchasing can be an effective partner in a competitive review process given adequate time and involvement in your requirement definitions.

In an effort to expedite sole source/brand requisition requests through purchasing, we would encourage you to review the criteria for Sole Source/Brand form herein. If you feel your request meets such criteria, follow the instructions in filling out the form and attach it to your requisition. If sole source/brand justification is warranted and accepted by Purchasing, the requisition will be processed for the sole source/brand as requested.

This is an internal review process. Departments are requested to use discretion in their discussion with vendors so as not to compromise any competitive advantage the Buyer may utilize, regardless of the acceptance or rejection of the sole source/brand justification.

Rather than merely a shift of the review process and burden, this process acknowledges the significant effort a department may undertake when identifying a vendor or brand, and provides you with the method by which to make your requisitioning efforts more efficient under sole source/brand conditions.

Purchasing will advise you when a particular competitive review process may both serve the County better and/or be required by governing law.

In order for us to accept a request for sole source/brand the certification, the form referenced herein should be made a part of your justification and be signed by an authorized department representative. This certification will remain on file as part of your requisition package for audit purposes.

SOLE SOURCE PURCHASING:

On rare occasions there may be a need to purchase goods or services from one vendor/contractor without going to formal bid or requesting competitive quotations. This is known as "Sole Source" purchasing.

"Sole Source" purchasing is authorized by Monterey County Code 2.32.040, Emergency Purchases, and by Monterey County Code 2.32.070, Competitive Bidding Not Required.

A sole source may be designated when it is apparent that a needed product or service is uniquely available from the source, or for all practical purposes, it is justifiably in the best interest of the County.

"Sole Source" purchasing may be necessary under certain circumstances such as an emergency wherein the department head or other County Official who is authorized to sign requisitions may purchase items for the continuance of the department function, or that items purchased are necessary for the preservation of life or property, and that no authorized purchasing department personnel are immediately available to make the purchase.

The designation of a "Sole Source" supplier must be authorized by the County Purchasing Agent or Deputy-Purchasing Agent before the requirement for competitive quotations is waived.

PROCEDURE:

Sole source/brand purchasing is an exception to the normal procurement function and requires a detailed justification. In processing sole source/brand requests for supplies, services and/or equipment, Purchasing adheres to and is governed by the principles set forth in both the Federal and State Laws governing public purchasing and the Public Contract Code, and by the adopted and approved County of Monterey Policies and Procedures. As such, our decision is final.

If you are requesting a particular vendor, brand or product, you must make this fact clear on your requisition. Such a request should not be made unless the request is reasonable and appropriately justified to meet legal requirements and can withstand a possible audit. The County requirements and the format for submitting such requests are contained herein. Please make copies of the Criteria for Sole Source/Brand form for your future use.

The following factors **DO NOT** apply to sole source/brand requests and should not be included in your sole source/brand justification. They will not be considered and only tend to confuse the evaluation process.

1. Personal preference for product or vendor
2. Cost, vendor performance, and local service (this may be considered an award factor in competitive bidding)
3. Features which exceed the minimum department requirements
4. Explanation for the actual need and basic use for the equipment, unless the information relates to a request for unique factors
5. A request for no substitution submitted without justification. This is a sole source/brand request requiring detailed justification including established sole source/brand criteria

County of Monterey
Contracts/Purchasing Department
JUSTIFICATION OF SOLE SOURCE/SOLE BRAND REQUEST

Purchase Requisition Number____________________ Date____________________

Description of Item: Carbon Black endpoint recording, customized detection, live response, remediation, and threat banning software

1. Please indicate the following:

Procurement: ■ Goods
■ Services

(Check One)

□ Sole Source: Item is available from one source only. Item is a one-of-a kind and is not sold through distributors. Manufacturer is exclusive distributor.

■ Sole Brand: Various sources can supply the specified model and brand and competitive bids will be solicited for the requested brand only. Meets form, fit and function- nothing else will do.

Note: Sole Source/Sole Brand Requests are not maintained as a standing request.
Each request is for a single one-time purchase only.

2. Vendor Selection:

■ Preferred Vendor
□ Sole Source

Vendor Name: KIS
Address: 48383 Fremont Blvd. #122 City: Fremont State: CA 94538
Phone Number: (510) 403-7576
Contact Person: Brad Goubeaux Title: Enterprise Account Manager
Federal Employer #: 68-0171024

3. Provide a brief description of the goods/services to be purchased and why this purchase is being proposed under a sole source acquisition.

a) Why were product and/or vendor chosen?

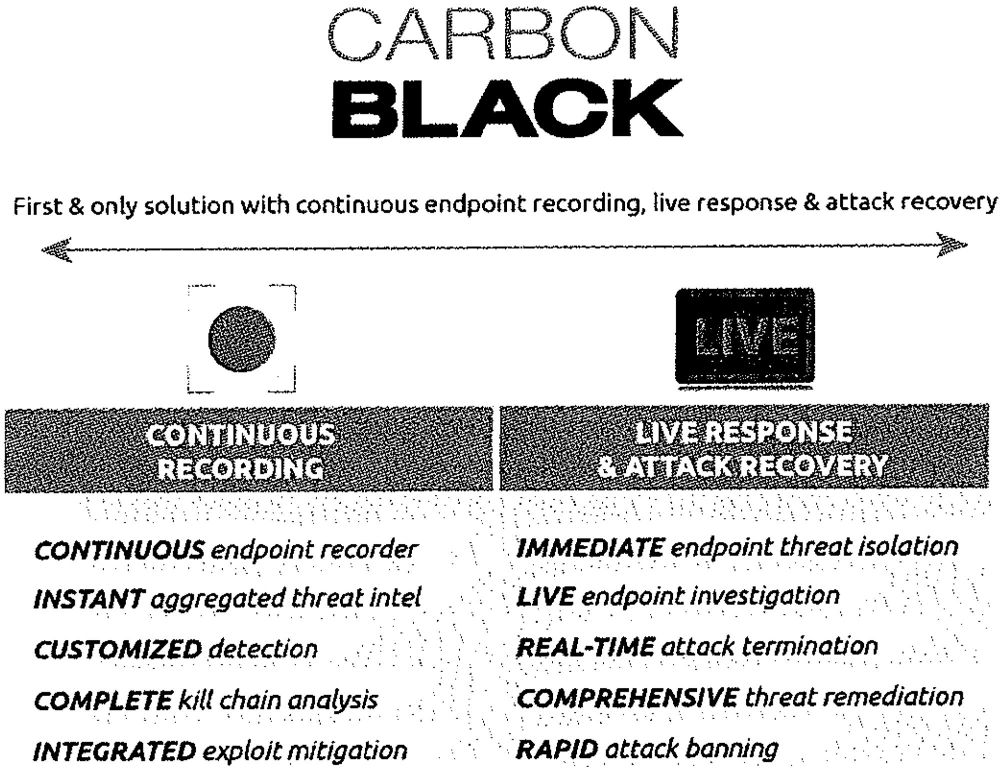
Carbon Black is a unique threat detection and data breach response platform, which will be used to secure County workstations, computers, laptops, and other mobile devices ("endpoints"). The Carbon Black security tool enables Security Operations Centers (SOCs) and incident response teams to prepare for a data breach through continuous endpoint recording, customized detection, immediate, live response to threats and data breaches, remediation of data breaches, and threat banning. Carbon Black makes threats easier to see and faster to stop by empowering SOC and incident response teams to arm their endpoints more effectively.

Carbon Black underwent a one-month proof-of-concept trial here at the County, and the results were very successful. Information Security Officers from each County department were impressed by its capabilities, including the ability for Information Security to respond to an endpoint incident more quickly and contain and isolate the system instantly using Carbon Black.

Three price quotes were obtained. Reseller was chosen based upon lowest price quote for the software and upon Reseller's agreement to the County's standard contract terms.

b) What are the unique performance features of the product/brand requested that are not available in any other product/brand? For Services: what unique qualifications, rights, and licenses does the vendor possess to qualify as a sole source/brand request?

As explained on the chart below, Carbon Black is currently the only product available that records all the activity that is occurring on a workstation and correlates it against known and malicious malware behavior. This feature instantly provides the County with the immediate opportunity to address a detected threat to the County network and information systems.



CARBON
BLACK

First & only solution with continuous endpoint recording, live response & attack recovery

CONTINUOUS RECORDING	LIVE RESPONSE & ATTACK RECOVERY
CONTINUOUS *endpoint recorder*	***IMMEDIATE*** *endpoint threat isolation*
INSTANT *aggregated threat intel*	***LIVE*** *endpoint investigation*
CUSTOMIZED *detection*	***REAL-TIME*** *attack termination*
COMPLETE *kill chain analysis*	***COMPREHENSIVE*** *threat remediation*
INTEGRATED *exploit mitigation*	***RAPID*** *attack banning*

c) **Why are these specific features/qualifications required?**

The County of Monterey currently has a system kill rate of between 50 to 75 computers per year, i.e., 50 to 75 computers must be shut down and isolated from the County network due to malware threats or penetrations. These "endpoints" are being compromised by advanced malware that bypasses anti-virus protections easily. Currently, when the threat is detected by existing County malware tools, Security is required to perform manual analysis on the affected endpoints in order to determine if the threat landed successfully. This can take several hours in many cases—time during which the threat may spread and may affect other systems or files to which the user has access.

In contrast, Carbon Black continuously records all actions of each County endpoint, so evidence of successful threat landings is already collected and can be instantly analyzed. Carbon Black's exclusive features enable Security to instantly understand the root cause of a malware threat (through Carbon Black's unique gapless recorded history and visualization of the entire attack kill chain). In this way, the Carbon Black security tool enables Security to respond and recover at the moment of discovery of a malware threat or penetration. In turn, the continuous information provided by the Carbon Black security tool enables Security to immediately "roll back the tape" to identify malware/threat root cause.

In addition, Carbon Black, unlike other security tools, allows Security to isolate the affected endpoint from the rest of the County network immediately upon malware threat or penetration, while it is being triaged. Endpoint isolation protects the rest of the County network, and the shared filesystems that the user has access to, from being infected by the compromised endpoint. The Carbon Black security tool uniquely allows County Security to remain connected with the Carbon Black server during a security incident. By maintaining an active connection with the Carbon Black server, even while the affected endpoint is isolated, Security is able to perform more conclusive investigations, both on and off the network.

The Carbon Black security tool also provides "endpoint threat banning," a function which would ban the hashes/signatures of identified malware on other systems in the County network. With the endpoint threat banning unique to Carbon Black, Security would be able to instantly stop, contain and disrupt threats from spreading in the County network, as well as block the future execution of similar attacks in the County network.

The Carbon Black security tool also provides malware "watch lists," which aggregates and provides intelligence on known malware threats. Through Carbon Black's proprietary watch lists, Security will have built for the County actionable detection by leveraging aggregated threat intelligence from the Carbon Black Threat Intelligence Cloud. This will enable Security to reduce alert fatigue by receiving and designing threat detection that is customized and optimized for the County.

d) What other products/services have been examined and/or rejected?

We were unable to find similar products with similar capabilities that are tailored to an organization of our size and type. The bulk of these capabilities are not part of any of our existing toolsets.

e) Why are other sources providing like goods or services unacceptable (please give a full meaningful explanation)?

Carbon Black is the number-one endpoint detection and response solution according to a SANS survey of incident response professionals. The SANS Institute is the foremost resource for the County of Monterey's Information Security Team for resources and training. Additionally, other California counties and members of the California Counties Information Systems Directors Association (CCISDA) are also turning to Carbon Black as a go-to solution for their data breach/malware incident response. The Carbon Black tool offers significantly more capabilities to protect the County network and information resources than other available products. Other products are "unacceptable" because, in the absence of the Carbon Black capabilities, they expose the County to significantly more risk of widespread data breach and malware penetration throughout the County network.

f) What are the unique performance features REQUIRED (not merely preferred), and how would your requirement be inhibited without this particular item or service?

See the answer to question c for detailed description of the Carbon Black features that are required in order to protect the security of the County network. The biggest current risk to

County information security is the current inability to immediately isolate infected endpoints and the inability to ban malware hashes on other systems. In the absence of ability to immediately isolate affected computers, malware can spread through the County network, while Security is undertaking manual investigation.

The Carbon Black tool's ability to ban malware hashes throughout the County network is essential to adequate network protection. Examples are the "Zeus" and "Blaster" outbreaks the County experienced in recent years. The ability to ban the hashes of these Trojans and worms, and thereby prevent them from spreading through the County network, would have saved the County the significant sums of money expended in cleanup work.

In addition, without the ability to ban malware hashes Countywide, Security's ability to respond to Cryptowall infections, in which County computers are disabled and/or County data is encrypted, for ransom, is limited. Failure to ban malware hashes, as the Carbon Black tool would permit, exposes additional risks to County data being destroyed through encryption by malicious actors.

Another unique feature of the Carbon Black product is the ability to generate digital footprints, as well as to correlate and document all the activities performed by a malicious actor (both external and internal) across the County network environment. This aspect of the Carbon Black tool would provide Security with the ability to see how many computers the malicious actors access as well as what actions they performed on those systems. This ability to observe and monitor malicious actor activity on the County network is essential to containing and stopping widespread damage to County information systems.

g) **Estimated Costs: $98,706.60 for the first year, $93,166.20 for two year thereafter, for a maximum of $285,039.00 over a period of 3 years.**

4. Is there an unusual or compelling urgency associated with this project?

☐ No
■ **Yes (Please describe)**

This year we are seeing an escalation in exploit kit attacks and ransomware attacks against County users and workstations. Attempts by websites to infect workstations with the dangerous Angler Exploit Kit are occurring on a daily basis. Dozens of successful attacks have already taken workstations out of service. Ransomware attacks are increasing worldwide, and the County has had three successful infections resulting in unrecoverable data. Ransomware is particularly concerning because the County won't pay ransom and critical data is lost with one click on the wrong phishing email.

While it is not possible to *prevent* all infections, the ability to isolate systems using Carbon Black and quickly determine the scope of an infection is invaluable to our containment efforts. The integrated exploit mitigation and threat remediation will help us significantly overcome the inadequacies of traditional anti-virus by allowing us to immediately halt a piece of malware from spreading or affecting a larger number of County computers. Having this tool in place as soon as possible will significantly help our malware fighting efforts. The ability to see how many computers the malicious actors access as well as what actions they performed on those systems, and to observe and monitor malicious actor activity on the County network, is essential to containing and stopping widespread damage to County information systems.

THE FOLLOWING TO BE COMPLETED BY THE REQUESTOR

I hereby certify that:

1. I am an approved department representative, and am aware of the County's requirements for competitive bidding, as well as the criteria for justification for sole source/brand purchasing.
2. I have gathered the required technical information and have made a concentrated effort to review comparable and/or equal equipment.
3. The information contained herein is complete and accurate.
4. There is justification for sole source/brand purchasing noted above as it meets the County's criteria.
5. A sole source/brand purchase in this case would withstand a possible audit or a vendor's protest.

4-12-16

Requestors Signature — Date

Dianah Neff — 4/13/16

Authorized Signature by Department Head — Date

4-26-16

Contracts/Purchasing Officer — *Date*