# INFORMATION SERVICES DEPARTMENT

168 N. Edwards St., PO Box 477, Independence, CA 93526
(760) 878-0398

Material or services to be delivered to:

Inyo County Information Services
Attn: Cybersecurity Bid
168 N. Edwards St., PO Box 477
Independence, CA 93526

**Bid Number:** IS-2024-08-12
**Bid Opening:** August 12, 2024
**Question Deadline:** August 30, 2024, 5:00 p.m. (PDT)
**Bid Closing:** September 30, 2024, 5:00 p.m. (PDT)

Prices quoted F.O.B. destination unless otherwise stated. Make your bid or quotation in the space provided on the attached sheets.

Any bidder who wishes their bid to be considered is responsible for making certain that their bid is received at the Information Services office by the bid submittal deadline. No oral, telephonic, telegraphic, or facsimile bids or modifications will be considered. Bids received after the bid submittal deadline will be rejected regardless of postmark date.

Questions must be sent to inyois@inyocounty.us with the subject line "RFP Questions IS-2024-08-12" and received no later than the Question Deadline. A document with the answers to all received questions will be posted no later than 10 days before bid closing.

IMPORTANT: The County reserves the right to reject all bids in its sole discretion and shall not be responsible for the cost of any bids submitted. Bid must be sealed with bid number as indicated above on the outside of the envelope. Read the Instructions and Conditions before making your Bid or Quotation.

**Instructions & Condition**

1. Any bidder who wishes to challenge the bidding or procurement process must file a complaint in conformance with Inyo County Code Chapter 6.30.
2. All prices and notations must be typewritten or written in ink. No erasures permitted. Mistakes

may be crossed out and corrections made adjacent to and must be initialed in ink by person signing quotation.

3. State brand or make on each item. If quoting an article exactly as specified, the bidder must strike out the words "or equal". If quoting on other than make, model or brand specified, the manufacturer's name and the catalogue number must be given, or descriptive cut and information attached to the quotations.
4. Quote on each item separately. Prices should be stated in units specified herein.
5. Each quotation must be in separate sealed envelope with bid number on outside, and must be submitted to Inyo County Office of Emergency Services, not later than the hour and day specified hereon, at which time it will be publicly opened and read.
6. Terms of less than ten days for cash discount will be considered as net.
7. All quotations must be signed with the Firm's name and by a responsible officer or employee. Obligations assumed by such signature must be fulfilled.
8. No charge for packing, drayage, or for any other purpose will be allowed over and above the prices quoted on this sheet.
9. The right is reserved, unless otherwise stated, to accept or reject any or all quotations, or any part thereof, either separately or as a whole, or, to waive any informality in a bid.
10. Samples of items, when required, must be furnished free of expense to the County of Inyo and if not destroyed by tests, will upon request be returned at the bidder's expense.
11. In case of default by the vendor, the County of Inyo may procure the articles or service from other sources.
12. Cost of transportation, handling, and/or inspection on deliveries, or offers for delivery, which do not meet the specifications will be paid for by the vendor.
13. The vendor shall hold the County of Inyo, its officers, agents, servants and employees, harmless from liability of any nature or kind on account of use of any copyrighted, or uncopyrighted composition, secret process, patented or unpatented invention, article or appliance furnished or used under this quotation.
14. The vendor will not be held liable for failure or delay in fulfillment if hindered or prevented by fire, strikes, or Acts of God.
15. Quotations are subject to acceptance at any time within ninety (90) days after opening same, unless otherwise stipulated.
16. Verify your quotations before submission as they cannot be withdrawn, or corrected, after being opened.
17. Amounts paid for transportation of property to the County of Inyo are exempt from Federal Transportation Tax. An exemption certificate is not required where shipping papers show the consignee as County of Inyo, as such, papers may be accepted by the carrier as proof of the exempt character of the equipment.
18. Small businesses and local businesses are entitled to contracting preferences in Inyo County. Please consult Inyo County Code Chapter 6.06 for details on these preferences.
19. All responses to this request are considered public records. Due to the County's obligations under the Public Records Act, any documents submitted to the County in connection with this request may by disclosed to any member of the public upon request.

# Introduction

The County of Inyo provides services to the nearly 20,000 residents of Inyo County with its 450 employees across 20 departments across multiple locations throughout many ifferent communities. Most of these locations are connected via a combination of a dark fiber network or leased network circuits to our two main locations in Independence and Bishop, CA.

The County delivers a range of services across these departments, some of which, such as the Sheriff and Corrections, offer 24/7/365 services, while others process payments and/or financial information from the public, e.g., the Treasurer-Tax Collector. Other departments, including Health & Human Services, handle highly sensitive data that fall under HIPAA compliance rules. In addition, the County is responsible for local election processes and has a significant set of security and compliance requirements.

Most of the County's application infrastructure is off-site (cloud-based SaaS) but, like most organizations, there are a few on-premises applications. There are also initiatives in place to potentially migrate additional functionality to hosted providers.

The purpose of this request for proposals (RFP) is to acquire services from a Managed Security Service Provider (MSSP) (or a variation which includes a Security Operations Center as a Service, a.k.a. SOCaaS) to complement the existing County resources and aid the County in protecting its digital assets. In doing so, County Information Service (IS) is seeking a partner or partners for the detection, review, analysis, and reporting of vulnerabilities and intrusion events, as well as assistance with the response to and recovery from such events.

# Solution Specification

Vendors can respond to one or both of the following sections based on their offerings. They may provide bundled pricing as an option, whereas a-la carte pricing (per each section A, and B, below) is required.

## A. Prevention and Protection

**REQUIRED AREAS**

a) Inyo County end points, servers, and users must be prepared and proactively protected against security threats.
   - Describe the proposed EDR solution and how it will keep track of evolving threats and known vulnerabilities.
   - Describe how priorities are assigned (e.g., Use CVE scoring) and the SLAs for patching.

b) Inyo County's public facing IT Infrastructure must be monitored for vulnerabilities through automated testing and the County staff must be provided with an evaluation report once a quarter.
   - Describe how such automated testing is performed, what vulnerabilities these tests look for and the format for the report.
   - Describe what kind of access is needed to perform such automated tests.

c) Inyo County IS expects regular updates and reports on key metrics in this area.

- Describe how the Service Provider would keep Inyo county informed of regular metrics, such as patches applied, whether SLAs are kept, any devices that the provider is not able to patch
- Describe if the County staff will have access to a dashboard showing all the county assets and the risk / current patching status.

d) Discuss the endpoint management solution proposed through this solution.
   - Describe if the solution provider can re-use existing County tools such as PDQ for managing endpoints; if not
   - What tools or solutions would be required and how will they be implemented, maintained, and costed

**OPTIONAL AREAS**

e) Work with the County staff for a full vulnerability and penetration test of internal and external resources including but not limited to networking equipment, on-prem and cloud (Azure) Infrastructure annually.Describe your needs for performing such a thorough annual evaluation and the outcome the county can expect from it.
   - Please specify if a free retest is included after 30 days to evaluate the fixes performed by the county staff.

## B. Incident Detection, Response, Recovery, and Reporting

**REQUIRED AREAS**

a) Must provide 24/7/365 security monitoring and alerting for endpoints, servers and network devices.
   - Please describe how this will be accomplished including the location of the staffing performing the monitoring during each time of the day.

b) The protection must prevent malicious code from running on any protected device.

c) SLA for notifying Inyo County of incidents.
   - Please describe the range of response/notification times available and associated costs
   - Describe how notification and escalation procedures would be provided appropriate for the criticality of the incident.
   - Please describe how the solution will validate events to reduce false positives, false negatives and how the criticality of events will be determined.

d) Must provide regular briefings to Inyo security team to keep them informed of the latest threats that could impact our organization.
   - Describe the methodology (email, call, in person), content and frequency of how this requirement would be met.

e) Indicate whether all services relating to monitoring, including those delivered by the third-party partners, will be available through a single portal.

f) Describe if there are any possible integrations between the solution and the Inyo County ticketing system (Freshservice), Windows Active Directory or other enterprise applications.

g) The Service Provider's Security Operations Center (SoC) must hold ISO27001 certification and be able to provide a SOC1 or SOC2 report.

- Please provide any other information regarding a third-party review of your organization's security practices.

h) The Security Operations Center must have 99.99% uptime. Onsite Security Analysts assigned to the Inyo County environment must hold a SANS GCIA certification or equivalent.
   - Additionally, please provide details around any initial and ongoing training of security monitoring staff.

i) Describe how the Service Provider would keep Inyo County informed of regular metrics, such as events analyzed, incidents detected, incidents handled by the services vs. incidents escalated to Inyo County, etc.

j) Inyo County IS staff expect to have access to data and the ability to perform queries or reports over the last 90 days of log data.
   - Discuss the options for a portal or similar for accessing information and performing these actions
   - If access to this tool is Internet facing, it must support SSO through M365.
   - Please describe if there are any limitations to this capability.

k) Must provide reporting capabilities, including the ability for Inyo County to request custom report types at no additional cost.
   - Describe how this is accomplished

l) Please describe how you detect and disrupt DoS attacks

m) Please describe how you detect and disrupt attempted and successful network intrusions

n) Please describe how you detect, isolate and recover compromised endpoints and network devices

o) Optionally, please describe how you detect and block anomalous LAN traffic

p) Please describe the level of support Inyo County can expect to receive from the security analysts in resolving incidents after Inyo County has been notified.

q) Please describe your 24/7 incident response services and how you charge for them.

**OPTIONAL AREAS**

r) Please describe how you provide full cycle security incident management: early detection, analysis, prioritization, notification, containment and forensics, recovery, and incident review, and how you charge for these services.

# Other Requirements and Vendor Information

**REQUIRED AREAS**

a) Describe how the solution will leverage security intelligence from other customers to detect potential events in the Inyo County environment.

b) Please provide the average years of experience for analysts that would be assigned to our account.

c) Please provide the % of staff which have security certifications and list those certifications.

d) Security analysts monitoring the Inyo County environment must have passed a background check prior to employment and must be in USA and checked annually.
    - Please elaborate on the process for screening and hiring security staff.
e) Please describe which components of the solution will be performed by personnel dedicated to Inyo County vs. which will be split among a pool of resources.
f) Please indicate the ratio of monitoring analysts to customers.
g) The proposer must designate one individual to function as the account representative to coordinate support and services related to the proposed.
h) Please include the cost of any additional software needed to perform these tasks in your quote.
i) Must provide contact information of three (3) referenceable clients. References from the public sector clients are preferred.
j) Please include documentation that demonstrates your experience in the field of managed security services.
k) Service providers should include the following information in their proposal:
    - The financial penalty owed should the service provider fail to meet SLAs described in the contract.
    - The method by which Inyo County will be reimbursed should a service which has been paid for does not meet the contractual expectations.
    - The financial penalty if the service provider is negligent in detecting a security event which causes the County damage.
    - Describe your processes and mechanisms for handling customer inquiries and reported issues, including SLAs.
    - Describe how all data gathered as part of the service will be kept confidential, and how it will be retained or destroyed at the end of the contract.
    - Describe how a copy of County data will be provided to the County at the end of the contract.
    - Describe the limitation of financial liability accepted by the service provider.
    - Please provide an explanation of the relationships between the service provider and any resellers or sub-contractors who would be dealing directly with the County, including how they will be held accountable for the services they provide.
l) Please explain whether incident response is provided by you or is outsourced. If outsourced, to whom exactly is it outsourced?
m) Is incident response managed and performed from the within the United States? If not, where is it located?
n) What onboarding guidance and assistance do you provide?
o) How is an incident response initiated?
p) Do you perform ad-hoc scans for zero-day vulnerabilities?
q) Would we have on-demand access to a comprehensive status dashboard, including of vulnerability assessments?
r) Are recovery services included? If so:
    a. Will there by a smooth, vendor-managed transition from the IR team to the Recover team?
    b. What is involved in the planning phase for recovery, and how long does it last?
    c. Is the ability to safely rebuild systems, including BIOS & firmware, included?

**OPTIONAL AREAS**

s) Develop a Recovery Plan: Establish a clear and detailed recovery plan that outlines the steps to restore operations, including prioritizing critical systems and data.
t) Backup and Restore: Regularly backup critical data and systems, and ensure that backups are tested and stored securely. Use these backups to restore affected systems during recovery.
u) Communication: Maintain clear communication with stakeholders, including employees, customers, and partners, about the status of the recovery process and any potential impact.
v) Post-Incident Analysis: Conduct a thorough analysis of the incident to identify root causes, lessons learned, and areas for improvement in security measures and response protocols.
w) Continuous Monitoring: Implement continuous monitoring to detect any residual threats or anomalies during the recovery phase.
x) Validation: Validate that systems and data are fully restored and functioning as expected before returning to normal operations.
y) Review and Update: Review and update the incident response plan and recovery strategies based on lessons learned and evolving threats.

# Inyo County Infrastructure

This section contains some helpful information that may aid in crafting a response.

| ITEM | ROUGH ESTIMATE |
|---|---|
| **General Scope** | |
| Users or employees | 450 |
| **External Scope** | |
| External IP addresses | 22 |
| Percentage of External IP addresses that are live | 50% |
| **Internal Scope** | |
| Internal IP addresses | 700 |
| Percentage of Internal IP addresses that are live | 100% |
| Networks or VLANs | 120 |
| Physical locations or branches | 2 main, ~20 other |
| | |

| | |
|---|---|
| | |
| **Web App Scope** | |
| Number of Custom Web Applications (eg. In-house built) | 5 (1 externally visible) |
| Custom vendor/native applications (eg. appliance sites) | 0 |
| **Wireless Scope** | |
| Wireless SSIDs | 3 |
| **Cloud Scope** | |
| Cloud Provider (AWS, GCP, Azure, Other) | Azure + M365 |
| Rough # of AWS/Azure Subscriptions or GCP Projects | 1 |
| Rough # of AWS/GCP VPCs or Azure VNets | n/a |
| **Mobile Scope** | |
| Custom mobile applications (and mobile system) | None |
| **Other Scope** | |
| Point of sale systems | n/a |

# Response Evaluation

Each response will be evaluated using the following scale:

| Criterion | Points |
|---|---|
| Provided a Compliant Response (pass/fail) | 10 |
| Detailed Complete Functionality within the Coverage Area | 20 |
| Demonstrated Experience and Success | 30 |
| Has Adequate Resources for Success | 20 |
| Offers responsive Support and Maintenance | 20 |
| **Total:** | **100** |

Although pricing is of paramount importance, you may notice that price is not one of the criteria listed above. Responses will be selected so as to maximize value, i.e., we will select the strongest response within the price range that we would be willing to afford.

The evaluation matrix above will be applied to each of the solution areas listed in the Solution Specification section, above.