**Inyo County Cybersecurity RFP IS-2024-08-12 - Q&A**

Updated: 9/13/2024

| No. | Question | Answer | Related Questions |
|---|---|---|---|
| 1 | How many end points are there, and how many servers? | There are around 550 end points and 50 servers (mostly VMs) | 61 |
| 2 | How many of Inyo County's 450 employees access IT systems? How many total users are there in the environment? | The IT staff is 12 people strong. Each of the 450 employees has an M365/Azure AD account, and there are about 50 additional group and machine (non-human) accounts. | 123 |
| 3 | How many people currently make up Inyo County's internal SOC team? How many architects and engineers? What is their experience level with MDR, EDR, and/or VM solutions/tools? | There are no full time cybersecurity personnel. There are 3 senior IT employees for whom cybersecurity is within scope. | |
| 4 | Please list all locations, including outsourced locations, that are in scope (e.g. primary locations, business units, data centers, call centers, data storage locations). | Primary: Bishop, Independence<br>Secondary: Tecopa... | |
| 5 | Is the management of each Inyo County site separate? If not, how are sites interconnected? | Not separate. Sites are connected by either:<br>- Site-to-site VPN over Internet (split tunnel)<br>- Site-to-site VPN over ELAN<br>- Dark fiber (switch to switch) | |
| 6 | Other than HIPAA compliance for Inyo's Health & Human Services department, are there other regulatory requirements and/or data segregation requirements? | Besides usual security best practicies, that is the only only regulatory requirement. | |
| 7 | What is the total number of assets that need to be monitored? | Approximately 650 (workstations, servers, FWs, and switches) | |
| 8 | Please provide an architecture diagram for each site or please define the architecture for each site, including: | N/A | |
| 9 | Number and types of network devices being monitored (e.g. access points, switches, IOT nodes) | See related question(s). | 1<br>61 |
| 10 | Total number of physical servers? How many are public facing? | Only one is public facing. Also see related question(s). | 1<br>61 |
| 11 | Number of LPARs (version of each), HA setup, modules, etc. | N/A | |
| 12 | Number of workstations (and operating systems) | Number of workstations: 450<br>Workstation OS: Windows 10 Enterprise | |
| 13 | What specific operating systems are present in the environment? What operating systems are feeding logs into the SOC? | Windows 10 and Windows Server (multiple versions) nearly universally. A few Linux (Ubuntu) servers. | |
| 14 | What is the current logging infrastructure architecture? What tool does Inyo use for log collection? | No SIEM or logger | |
| 15 | What is the current daily log volume ingested (range)? Please specify. | N/A | |
| 16 | Other than PDQ Detect, what other tools does Inyo County use for MDR? | ESET and Albert | |
| 17 | What are the SOC data retention requirements for each site (in years)? | TBD | |
| 18 | If data retention requirements are due to a specific compliancy or regulation, please list requirements per site. | TBD | |
| 19 | Is the objective for the MSSP to fully manage the SOC or is Inyo County looking for a hybrid/co-managed solution? | The SOC is to be fully managed by the MSSP | |
| 20 | Is Inyo County currently mapping to any existing cyber security frameworks (e.g. NIST, ISO27001, MITRE ATT&CK)? | NIST 800-53 | |
| 21 | Does Inyo County subscribe to any threat intelligence feeds? | Yes, including but not limited to federal and state sources. | |
| 22 | Does Inyo County currently use any SOAR technologies and/or have SOAR requirements? | No. | |
| 23 | Does Inyo require any on-site support for MDR? | No. | |
| 24 | How many total endpoints are in scope? | See related question(s). | 1<br>61 |
| 25 | What tools does Inyo currently use for EDR/endpoint management/protection? | ESET, Intune, and PDQ Deploy/Inventory | |
| 26 | For EDR, is the management of each Inyo County site separate or are all sites managed by a single S1 management instance? How are sites interconnected? | See related question(s). | 5 |
| 27 | Does Inyo require any on-site support | No. | |
| 28 | What tools does Inyo currently use for Vulnerability Management (VM) and scanning? | We employ an external service to perform scanning and provide a comprehensive report. | |
| 29 | Does Inyo County have established scanning windows? | No. | |

| | | | |
|---|---|---|---|
| **30** | Does Inyo County have an asset management tool? If yes, what tool? | We have modules in our ERP system as well as in our IT ticketing system (FreshService). | |
| **31** | How many assets does Inyo County have connected to its internal network? | Approximately 550 (plus ~ 300 mobile) | |
| **32** | Please provide the breakdown of assets (servers, workstations, network, etc.). | See related question(s). | 61 |
| **33** | Are there are any CMDB integrations needed? | No | |
| **34** | Does Inyo County currently perform scans on its internal network? At what cadence? | No | |
| **35** | How many of Inyo County's assets are exposed externally to the internet? | Excluding firewalls, 6 assets are exposed to the Internet. An additional 4 are exposed indirectly via proxy. | |
| **36** | Does Inyo County currently perform scans on its external network? At what cadence? | Yes, at least annually. | |
| **37** | Does Inyo County intend to scan assets in cloud environments and/or third party service providers? | No | |
| **38** | Does Inyo County have VM agents deployed? | No | |
| **39** | Does Inyo County have defined SLAs for remediation? | No | |
| **40** | How does Inyo County define remediation and contrast that to response? (For example, isolating hosts is considered as response, but patching an exploited vulnerability or reimaging a workstation is considered as remediation.) | Response: Form incident management team, notifify Inyo countacts, investigate and isolate.<br>Remidiation: Necessary patching/reimaging, data recovery, prevention (post mortem) | |
| **41** | Does Inyo County intend to dedicate internal personnel to its Vulnerability Management program? | Yes | |
| **42** | Are there any testing window restrictions for either assessment? | Yes; testing windows must be coordinated in advance, especially when the testing touches public safety and other critical functions. | |
| **43** | Are there onsite requirements for penetration testing? | No | |
| **44** | How many physical locations need to be assessed? | Two | |
| **45** | Thoroughness<br>☐ Manual – Most comprehensive assessment leveraging the best tools, but consisting mainly of manual review (80% manual, 20% tools).<br>☐ Automated – Appropriate for a lite-weight assessment where budget or time are restricted and manual effort is not desired. | Manual | |
| **46** | Are any in-scope nodes hosted with a third-party cloud provider? If yes, which? | No | |
| **47** | What level of information sharing does Inyo County want to provide?<br>☐ Semi-Blind (provide IP ranges and hostnames only)<br>☐ Hybrid (have vendor identify target ranges and fill in any gaps prior to the assessment) | Hybrid | |
| **48** | What level of evasiveness should the vendor employ?<br>☐ Non-Evasive<br>☐ Hybrid-Evasive | Hybrid-evasive as long as it is non-disruptive to County systems. | |
| **49** | Can access be provided such that all in-scope systems are reachable from a single network location? If no, please describe | Yes | |
| **50** | Are the annual assessments being conducted to fulfill PCI-DSS compliance requirements? | No. PCI-DSS is out of scope. | |
| **51** | Will any other ISO Certifications [other than 27001] be considered? | Additional relevant certifications include ISO 27016 and 27017, as is SOC 2 Type II. The County is looking for providers who have taken the time to create robust processes and have them reviewed and approved by an independant 3rd party. | 52 |
| **52** | If a provider is ISO27001 certified, and providing services to other California Counties, but does not have a SOC 2 report will the County consider them for response? | Yes. The intent is to have at least ISO 27001 or SOC 2 Type II, at minimum. Having both is better, as is having additional certifications. | 51 |
| **53** | In the case of a prime/sub vendor team, can the certification requirements be held by either the prime or sub and be considered as compliant? | The response is complient as long as the identity of the sub is known to the County and the County may, at its discretion, contact the sub directly. | |
| **54** | Is Inyo County planning on having the Managed Security Services Provider patch all IT systems? If so, what Operating Systems need to be covered? | The County can deploy patches based on guidance from the MSSP, i.e., direct patch management is desirable but not required | 57 |

| | | | |
|---|---|---|---|
| **55** | If an MSSP provides licensing and tooling for the customer to deploy the security tools but does not manage them directly through a tool like PDQ, would you still be interested in a response for Section A? | Yes | |
| **56** | Does the County want to have Vulnerability Management-as-a-Service included in the response and quoted? | Yes | |
| **57** | If so, what level of service would the Count like to have quoted, Scanning & Reports or Scanning, Reports and Patching? | Scanning & Reports as a minimum, with patching as an optional enhacement | 54 |
| **58** | For the Optional Areas; Does the county want to receive quotes for these optional services or just confirmation that the responder can provide these services? | Yes, please quote the optional services if you would like the County to consider purchasing them from you. | |
| **59** | If the county would like to receive quotes for Backup and Restore, what is the total data quantity expected to be backed-up and restored? | Backup and restore is not within the scope of this RFP. If you consider B&R to be integral to your offering, the amount of mission critical data to back up is only 500GB. | |
| **60** | For 24x7 SOC/MDR, which security tools/log sources are in scope for ingestion into the SIEM? | Switches and firewalls. Potentially the endpoints as well. | |
| **61** | **Please include vendors and quantities:** | | 1 |
| **61a** | Firewall vendor | 20x Fortinet | |
| **61b** | EDR vendor | ESET | |
| **61c** | On-prem and cloud environments | M365, Microsoft Azure, On-prem Windows, multiple SaaS | |
| **61d** | Workstations | 550x Windows workstations | |
| **61e** | Servers | 50x Windows servers (mostly VMs) | |
| **61f** | Switches | 35x Alcatel-Lucent switches | |
| **62** | Are you using a SIEM tool today? If so, what is your current ingest? | No | 76 |
| **63** | "Onsite security analysts" - Is the expectation for on site (i.e. in person) SOC analysts from MDR vendor to Inyo? | No. There is no requirement for the vendor to have analysts on site at the County of Inyo. | |
| **64** | Are fully USA Based analysts a hard requirement? Or is it just data residency in the USA? (This is important to note due to cost of staffing USA only analyst). | Data residency in the US is a hard requirement. US-based analysts is a very strong requirement. The County will consider (but reserves the right to reject) submissions in which the analysts reside in countries strongly allied with the US. | 69<br>71 |
| **65** | Are we allowed to submit multiple offers? | Yes | |
| **66** | When submitting multiple offers, in separate envelopes, do we submit separate copies of services documentation as well? | For efficiency, you may incorporate those sections by reference, as long as the reference is uambiguous (provide the precise name of the document we should be looking up, and where we would find it). | |
| **67** | Is there a page limit to the bid? | No. There is no requirement for the vendor to have analysts on site at the County of Inyo. | |
| **68** | Is the county also interested in XDR solutions? | Yes | |
| **69** | Is there a requirement for a US based only SOC? | Yes, although we would consider a SOC based on a country closely allied with the US. | 64<br>71 |
| **70** | Does Inyo County require SOC2 report to be included in the bid submission? | No, but we may request to see it as a part of our vetting process. | |
| **71** | All US client traffic stays in the US unless all US SOCs go down or everybody is handling an incident then it will go to one of our non-US SOC. Can we still respond to this RFP? | Yes, as long as you specify where the non-US SOCs are (to ensure they are in countries closely allied with the US), and you submit all employees to regular and robust background checks. | 64<br>69 |
| **72** | What Microsoft license does Inyo have? E3, E5, G3, G5, etc.? | G3 | |
| **73** | Does Inyo have Microsoft Defender today? | Yes | 95a |
| **74** | Are all the subnets visible from one location? If not, how many locations need to be accessed to see all subnets? | N/A | |
| **75** | You request an SLAs for patching. It's not customary for Managed Security Services Providers to perform patching as this is handled by the infrastructure support teams. MSSPs customarily provide recommendations for patching. Do you want SLAs for patching recommendations? | Yes | 54<br>57 |
| **76** | Does Inyo have a SIEM in place today? If yes, what is your average log ingest rate per day or per month? | No | 62 |
| **77** | In item B(h), does "Onsite" mean at the supplier's location? | Yes (it does not mean at the customer's location) | |

| | | | |
|---|---|---|---|
| **78** | This question is regarding this requirement: "l) Please describe how you detect and disrupt DoS attacks." Does this imply that the bidder should include a network-based DDoS mitigation service in the solution proposal? | Yes, if that is a part of your offering. | |
| **79** | Please provide a list of network devices showing make and model. | See related question(s). | 61 |
| **80** | Please provide information about the servers: quantity, operating system, and whether physical or virtual. | See related question(s). | 1<br>61 |
| **81** | We hold certification as a SSAE 16 Service Organization Contril (SOC) 2, Type II Attestation however we do not hold certification in ISO27001 as that tends to be for manufactures. Will our proposal still be considered without an ISO27001 certification? | Yes | 51<br>52 |
| **82** | **We understand that you may not want to give specifics due to this being publicly available. If you cannot give us the brand of a tool, would you be able to tell us if you use that type of tool. (IE 2 Firewalls, 1 MFA tool, 2 Email tools, etc.)** | | |
| **82a** | Do you require your data to stay within the United States | Yes | |
| **82b** | Number of Servers | See related question(s). | 61 |
| **82c** | Number of Firewalls | See related question(s). | 61 |
| **82d** | Number of IoT/OT | None | |
| **82e** | Number and brand of firewall | See related question(s). | 61 |
| **82f** | Number and brand of SD WAN | None | |
| **82g** | Do you use Cisco ISE | No | |
| **82h** | Number of Core Switches | See related question(s). | 61 |
| **82i** | Number Network Threat Analytics (Darktrace, Stealthwatch, etc.) | Albert | |
| **82j** | Brand of MFA/Identity | Azure AD/Entra ID | |
| **82k** | Brand of Cloud Web Security (Umbrella, Prisma Cloud, etc.) | Fortigate | |
| **82l** | Brand of Email Security Tool | MS Defender | |
| **82m** | Brand of Deception Technology | None | |
| **82n** | Brand of Workload protection (Tetration, Illumio, etc.) | None | |
| **82o** | # of vCenters | None | |
| **82p** | # of Virtual Cloud Directors | None | |
| **82q** | # of Nutanix Prism Instances | None | |
| **82r** | # of Domain controllers | None | |
| **82s** | # of servers under compliance | N/A | |
| **82t** | # of standalone DNS, DHCP, Certificate, NPS, Radius, Etc. | See related question(s). | 61 |
| **82u** | # of On-premise email servers | None | |
| **82v** | # of Public facing servers | 1 | |
| **82w** | # of of Any servers you want watched closely | ~10 | |
| **82x** | Brand of Privileged Access Management (CyberArk, Thycotic, Beyond Trust, etc.) | BeyondTrust | |
| **82y** | Backup Service (Veeam, etc.) | None | |
| **82z** | Brand/Type of any other security tools (Horizon3, Netwrix, Varonis, etc.) | None | |
| **83** | How many live hosts/assets will be covered by the solutions needed in Section A? | See related question(s). | 1<br>61 |
| **84** | Is there an incumbent EDR solution or endpoint management solution? If so, which vendor? | ESET | 61b |
| **85** | Can bids proposals be submitted electronically and if so, to where? | No, proposals must be mailed in per the instructions. | |
| **86** | Do all SOC staff and employees have to be located in the U.S. or can part of the team (front line analysts) be located in the U.S. SOC with support from global team/SOC? | See related question(s). | 64<br>69<br>71 |
| **87** | Are you interested in social engineering assessments such as phishing, as the number of employees was included? | Yes, as long as the solution is integrated with Outlook (web- and app-based) and includes user training on how to spot phishing. | |
| **88** | For the network VLANS, do you have one subnet that can see all subnets for a complete vulnerability assessment? | Yes | |
| **89** | If there is only one central subnet, how many different networks would be needed for a complete scan? | N/A | |
| **90** | Are you looking for physical security assessments? If yes, how many buildings would be in scope? | No. | |
| **91** | Are all five web applications in scope for a web application penetration test? | No, only one because it is externally visible. | |

| | | | |
|---|---|---|---|
| **92** | For the wireless security assessment, are you open to providing a laptop that can be used remotely for testing? | We would need to understand more about this request to provide an answer. The concern is not the hardware but the access privileges this laptop would have. | |
| **93** | For the cloud Scope, do you consider that internal for purposes of a pentest? | No. | |
| **94** | Do you also want a cloud configuration assessment (Assess against STIG or CIS benchmarks) | As a future option, yes. This is not required today but will help us select an offering that is future-proof. | |
| **95** | **EDR Questions:** | | |
| **95a** | Is there currently an EDR solution (e.g., CrowdStrike, Symantec, Microsoft Defender) deployed in the environment? | ESET and Microsoft Defender. | 73 |
| **95b** | Should the service provider integrate with this existing EDR solution, or is a new EDR solution expected as part of the proposal? | We are open to either option. | |
| **96** | **Vulnerability Management Questions:** | | |
| **96a** | Are there any vulnerability management tools (e.g., Qualys, Tenable, Rapid7) currently in use? | No | |
| **96b** | Should the service provider use these existing tools for vulnerability scanning and reporting, or is the provision of a new solution required? | See related question(s). | 95b |
| **97** | **SIEM Questions:** | | |
| **97a** | Is there a SIEM tool (e.g., Splunk, IBM QRadar, LogRhythm) already deployed for log management and security monitoring? | See related question(s). | 62<br>76<br>103 |
| **97b** | Should the service provider utilize the existing SIEM platform for incident detection and response, or propose a new SIEM solution? | N/A | |
| **98** | **Endpoint Management Questions:** | | |
| **98a** | Are there tools like PDQ, SCCM, or Jamf currently in place for endpoint management? | We have PDQ. | |
| **98b** | Is the expectation that the service provider will manage endpoints using these tools, or should they propose an alternative management solution? | See related question(s). | 95b |
| **99** | **Patch Management Questions:** | | |
| **99a** | What tools (e.g., WSUS, Ivanti, Automox) are currently used for patch management in the environment? | PDQ | |
| **99b** | Should the service provider integrate with these tools, or provide a new patch management solution? | If possible, provide both of these options. If not possible, provide what you have. | |
| **99c** | What is the breakdown of endpoints and servers in the environment? | See related question(s). | 1 |
| **99d** | What is the breakdown of the OS in the environment? | See related question(s). | 13 |
| **100** | When you discuss vulnerability scanning services, do you also require application scanning or just infrastructure? | Infrastructure and one externally-visible application. | |
| **101** | Does the County have an EDR solution in place today? If so, do they wish to keep that solution or are they open to the service provider to recommend one? | See related question(s). | 95b |
| **102** | Can city provide the number of assets they want to be protected by EDR and their type / distribution (example, mobile iOS devices, Windows Servers, etc) | See related question(s). | 1 |
| **103** | Does the County have a SIEM/SOAR solution in place today? Are they open to the service provider to propose one? | No, and we are open to have the provider propose one. | 62<br>76 |
| **104** | Does the County employ other preventative measures such as Firewall and IPS systems? If so, can you identify other preventative technologies in scope of monitoring | Yes, we use firewalls with IPS capabilities. | |
| **105** | Does the County require incident response service including eradication and containment of security threats or is this a hybrid function. Meaning, the service provider is to work with the The County IT team to accomplish the incident response? | Yes | |
| **106** | Is the County open to have an international SOC monitoring team using the SOC hosted within the US? | Hosted within the US. | |
| **107** | Can the County please provide the PDQ modules in use today? | Deploy, Inventory, and Connect | |
| **108** | Is there an electronic submission process for this RFP? Instructions look to be United States Postal Service (USPS) hard copy mail. | See related question(s). | 85 |

| | | | |
|---|---|---|---|
| **109** | Would the County be open to comparable certifications in lieu of ISO 27001? | See related question(s). | 51<br>52 |
| **110** | Page 4, Sec A, Sub d, first bullet: integrate with PDQ endpoint monitoring/management. Is this an absolute? | No | |
| **111** | Page 4, Sec B, Sub a, first bullet b: prevent malicious code from running on any protected device. We don't believe this is possible. Prevention is the goal. Is this an absolute? | Prevention is the goal, correct. | |
| **112** | Page 4, Sec B, Sub g: ISO 27001 certification and SOC 1 or 2 report. Are these absolute? | See related question(s). | 51<br>52 |
| **113** | Page 5, Sec B, Sub h: SANS GCIA certification. Are these absolute? | Yes | |
| **114** | The RFP instructions state "each quotation must be in separate sealed envelope". Are we able to provide our response via email instead or is a physical copy required? | Physical copy is required. | |
| **115** | Are you looking for a Service Provider solution delivery model (non-dedicated staff) or are you looking for on-site or "staff augmentation" model to provide services. | Either option works. | |
| **116** | Would you be willing to separate the cyber security functions from the IT operations functions (endpoint management, patching, backup, restore, rebuild) and have these provided by different providers? | No. In a time sensitive situation, it is best for a single team to handle all of this. | |
| **117** | What is the budget for this project? | We will be using Federal/State grants along with county contributions. We will consider the value delivered and what other rural california counties are paying for similar services when making a decision. | |
| **118** | If the proposed solution that meets all the "required" components exceeds budget, would a reduced scope be considered? | Yes | |
| **119** | Typically, organizations will accept either an ISO27001 or SOC2 Type 2 certification, which covers similar controls. Will you consider proposals from vendors with only an ISO27001 certification? | See related question(s). | 51<br>52 |
| **120** | **For each major site:** | Bishop / Independence | |
| **121** | What is the quantity and speed (Ingress/Egress) of the Internet circuit(s) servicing this location? | 200 Mbps symmetrical / 200 Mbps symmetrical | |
| **121a** | How many users are at this location? | 200 / 150 | |
| **121b** | How many servers are at this location? | Bishop: 32<br>Independence: 18 | |
| **121c** | # and types of Physical servers? | Bishop: 3 (Nutanix/Linux - virtual hosts)<br>Independence: 11 (Windows) + 1 (Linux) | |
| **121d** | # and types of Virtual servers? | Bishop: 25 (Windows) + 4 (Linux)<br>Independence: 1 (Windows) + 5 (Linux) | |
| **121e** | What are you utilizing for a virtualization platform | Nutanix / Hyper-V | |
| **121f** | Firewall | Fortigate / Fortigate | 61 |
| **121g** | How many are deployed? | 1 / 1 | 61 |
| **121h** | Are they configured in an active/active or active/passive configuration | NA - both sites have a single, independent firewall. Failover routes exist to send one site's traffic to the other site's firewall if necessary. | |
| **121i** | LAN Switch | Alcatel-Lucent | 61 |
| **121j** | Does the Switch support a Mirror/SPAN interface for traffic monitoring? | Yes | |
| **121k** | Type and speed of Mirror/SPAN interface? | SFP+ (10 Gbps) or QSFP28 (100 Gbps / 4x 25 Gbps) | |
| **121l** | Coper, Fiber (MMF/SMF), Twinax? | Depends on SFP module used | |
| **121m** | Do the Departments access the Internet through a single location, i.e. Bishop or Independence or do some County Departments have their own internet service and do not access the internet through the Main Locations? If applicable what is the quantity internet circuits and speed of the respective County Department's internet service? | Most departments access the Internet via one of the two main sites (Bishop and Independence).<br><br>Approximately 10 sites have their own Internet connections, typically with speeds of around 30 Mbps down and 5 Mbps up | |
| **122** | Can you provide per-department information? | This is not relevant, because IT is centralized across all departments. | |
| **123** | Number of M365 users? | 450 users, 550 total accounts | 2 |
| **124** | Cloud servers (AWS/Azure/GCP)? | None. | |
| **125** | Are servers on-premises or co-located? | On-premises. | |

| | | | |
|---|---|---|---|
| **126** | Are any of these Azure log sources enabled:<br>•Entra ID License?<br>•Azure Defender for Cloud?<br>•Microsoft Defender for Identity?<br>•Azure Activity Log?<br>•# of Azure Resource Groups? | None. | |
| **127** | Are any of these other log sources enabled:<br>•Identity Access Management (IAM)/Authentication?<br>•Firewall/UTM?<br>•AV/Endpoint/EDR?<br>•AV/Endpoint/EDR #2?<br>•Security Service Edge (SSE)?<br>•Proxy?<br>•VPN?<br>•Wireless Access Points?<br>•DNS?<br>•MFA/2FA?<br>•Email Security?<br>•Other? | Entra ID logs for authentication and MFA<br>Firewalls log locally and to Forticloud<br>AV/EDR logs to ESET Cloud<br>Wireless APs log to Juniper Mist Cloud<br>Email logging via Exchange Online<br>VPN server logs locally | |
| **128** | Does the County require more than 90-days of log retention? | No. | |
| **129** | Does the County do anything for Log aggregation? | No. | |
| **130** | Does the County utilize a SIEM? | See related question(s). | 62<br>76 |
| **131** | Does the County have cyber insurance? | Yes. | |
| **132** | Does the County have a preferred EDR solution, or are you seeking the MSP's recommendation? | Seeking the MSP's recommendation. | |
| **133** | We see 450 users, but what is the device count to be protected by the EDR solution? | 550 endpoints and 50 servers | |
| **134** | If different from the EDR solution, what device count will the patch management solution will protect? | 550 endpoints and 50 servers | 54<br>57 |
| **135** | What PDQ tools does the County utilize, and do you wish to stay with PDQ or look at an alternative solution? | We are happy with PDQ, but if there is a compelling reason to use something else, we are open-minded. Also see the related question. | 107 |
| **136** | Does the County currently have a backup system in place? If yes, what is the solution? | No. | |
| **137** | If not, how many terabytes of data would be backed up, and what is the required retention? | See related question(s). | 59 |
| **138** | Does the County maintain a golden image of its workstations and or servers? | The County is in the process of switching to Microsoft Autopilot for imaging. | |