National Trust for Historic Preservation
Save the past. Enrich the future.

Addendum No. 1

PROJECT: MANAGED SERVICE PROVIDER

DATE: JUNE 5, 2026

RE: ADDENDUM NO. 1 TO REQUEST FOR PROPOSALS, ISSUED MAY 18, 2026

TO: ALL BIDDERS

This addendum forms a part of the Contract Documents and modifies the original Bidding Documents dated May 18, 2026, and shall be included in the relevant scopes of work and bids submitted. It is the bidder's responsibility to determine if their work is affected by this addendum. Failure to acknowledge receipt of this Addendum on bid submission may subject the Bidder to disqualification.

The Following is AMENDED:

GENERAL NOTES AND CLARIFICATIONS:

1. Responses to questions received from Contractors is attached. Questions submitted that were deemed irrelevant to the RFP or beyond the scope of information required to submit a proposal were omitted.

SPECIFICATIONS: We would like to correct the RFP regarding the following: There are 6 servers in Azure, not 5 as indicated in the original RFP document.

END OF ADDENDUM NO. 1

600 14th Street NW Suite 500 Washington, DC 20005
E info@savingplaces.org P 202.588.6000 F 202.588.6038 **SavingPlaces.org**

RFP 2026-6 Q&A Document for Managed Service Provider

Q1. Is the current IT provider managing and hosting the 5 Azure servers, or are you directly paying through Microsoft?
R: We directly pay through Microsoft.

Q2. If the Azure servers are hosted in the Azure cloud, could you please provide the specifications for each individual server, including: RAM, CPU, HDD?SSD storage?
R:

- **COLOMGMT – RAM 8 GiB, VDPU 2**
- **AzureDC01 Standard B2ms, VCPU 2 RAM 8 Gib**
- **AzureDC02 – Standard D2s V3, RAM 8Gib**
- **COLOSRV1 – Standard D4as v4, VCPU 4, RAM 16 Gib**
- **Terminal – Standard D4s v3, VCPU 4, RAM 16 Gib**
- **Timeslips – Standard E2s v3, VCPU 2, RAM 16 Gib**

Q3. Are the Veeam backups currently covering any on-premises servers? If yes, how many?
R: Veeam is currently covering 6 on-premises servers. Please note that we are under contract for backups until next June. However, it is helpful to know what backup solution your organization offers.

Q4. Is the Microsoft 365 environment also being backed up?
R: No, but we have plans to add this in the coming months.

Q5. How many total servers are currently being managed within the environment?
R: Six servers are being managed in Azure.

Q6. Could you please clarify what the Mac server in the environment is currently being used for?
R: The Mac server is being used to store documents created by our Creative team. However, this server will be decommissioned in July. All Mac files are being migrated to Dropbox.

Q7. What services and applications does the Mac server support?
R: The Mac server is being decommissioned. However, it currently supports 3 creative team users and supports our magazine staff.

Q8. Can you provide a ticket report that shows tier 2 and 3 tickets for the last 6 months? Or at least an estimate on how many tickets monthly fall into those categories?
R: Most tickets are handled by our internal IT Team. I would estimate that 3-5 get submitted to our MSP monthly.

Q9. Do you plan on keeping Okta in place? Are there any other technologies from the stack listed that will remain in place for the incoming MSP?
R: Okta will remain in place. The National Trust pays for and manages Okta.

Q10. What is your current Microsoft licensing count? Can you please provide the license renewal dates?
R: Business Premium – 292 licenses, Business Basic 272 licenses

Q11. For the assigned technical consultant, how do you define meeting regularly with your IT team? Can you provide an idea of cadence (hours per month)?

R: We currently have weekly meetings scheduled; however, meetings depend on need. I would say we average 2 meetings per month with each meeting being 1.5 hours.

Q12. Are there any planned IT projects or initiatives that NTHP is looking to start in the next 12 months that would involve the new MSP?
R: Implementation of Microsoft Defender. However, this may be completed before our current contract expires.

Q14. Is Veeam Backup and DR licensing owned by the current MSP or by NTHP?
R: We purchase Disaster Recovery as a Service from our current MSP.

Q15. Is the Zoom phone system in scope for support by the MSP?
R: No, NTHP fully supports our Zoom phone system.

Q16. Can the National Trust provide an inventory of SonicWALL firewall models and firmware versions across all locations so that respondents can assess end-of-life/end-of-support status and plan accordingly?
R: TZ370 – 11
TZ270 - 1
NSA2700 – 2
Azure-NSv470 – 1
None of our firewalls are end of life.

Q17. Is the Mac Server at the DC headquarters used solely for backup, or does it serve additional functions (file sharing, directory services, etc.)? Should it be included in the managed services scope?
R: The Mac server is used for backup and file sharing. This is being decommissioned and all files are moving to Dropbox.

Q18. Are Veeam backups currently managed on-premises, in Azure, or through a third-party Backup-as-a-Service provider? What is the current backup retention policy?
R: Veeam backups are managed by our MSP.

Q19. What is the current Disaster Recovery as a Service (DRaaS) platform, and what are the target Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for critical systems?
R: Recovery Time Objective – (4) hours
Recovery Point Objective – (8) business hours
One annual disaster recovery test and up to 3 automated Disaster recovery tests.

Q20. Does the National Trust anticipate the ~305 endpoint count remaining stable over the initial contract term, or should respondents plan for growth or contraction?
R: The count will remain stable.

Q21. Are Microsoft Sentinel and Microsoft Defender managed by the current MSP, by NTHP internal staff, or by a separate security vendor? Should SIEM/XDR management be included in the MSP scope?
R: Sentinel is managed by the current MSP. Defender is not implemented, but NTHP manages the licensing.

Q22. What is the current Windows operating system version distribution across the 300 Windows endpoints? Are these under warranty? Laptops or desktops?

R: Windows 11. Most are under warranty. Our environment has mostly laptops with some desktops being used at our Historic Sites.

Q23. For the five internal NTHP IT staff referenced in the RFP, which support functions will they retain (e.g., Tier 1 help desk, Okta administration, SharePoint management), and which functions should the MSP fully assume?

R: Our internal staff handle most of our operations. We handle all Help Desk calls but will escalate if needed (basically Tier 3). We handle all Okta administration and Sharepoint management. MSP would handle some patching (we are currently implementing Intune). Backups are handled by current MSP until June 2027.

Q24. Should the MSP provide after-hours and weekend support coverage, or is standard business hours support with emergency-only escalation outside of business hours acceptable?

R: We require standard business hours with emergency only escalation. Security monitoring needs to be 24x7x365.

Q25. Is SharePoint administration and support fully retained by NTHP, or are there any SharePoint-related tasks the MSP should account for (e.g., migration assistance, security configuration, backup)?

R: While NTHP does fully administer SharePoint, we do occasionally need assistance from our MSP. It is important that the MSP has SharePoint capability as we plan to redo our SharePoint offering in the future.

Q26. Which and how many Microsoft Licenses are used by NTHP?

R: Business Premium – 292 licenses, Business Basic 272 licenses

Q27. Are there any third party services that have not yet been mentioned that are part of the IT Environment, or network, or need to be supported by the MSSP or considered in the network? Voip? iOT? OT? Cameras?

R: No. All third-party applications are currently handled by internal IT staff.

Q28. Will the incumbent MSP be contractually obligated to participate in a structured knowledge transfer during the transition period, or should respondents plan for a scenario where the outgoing provider's cooperation may be limited?

R: The incumbent MSP will participate in a structured knowledge transfer during the transition period.

Q29. Can the National Trust provide a current network topology diagram and asset inventory to prospective respondents, or should respondents assume a discovery/audit phase as part of the onboarding scope?

R: Assume a discovery phase as part of the onboarding scope.

Q30. Is there a preferred go-live date or hard deadline for the transition to be complete following contract award (anticipated July 15, 2026)?

R: Our current contract ends at the end of October. Hard deadline would be October 30, but I would prefer that most work be done earlier than this. I prefer for this to be completed in early October.

Q31. Is the National Trust open to multi-year agreements (3-year or 5-year) with commitment-based discounts, or is a 1-year initial term with renewal options preferred?

R: We are open to a multi-year agreement.

Q32. The RFP references "discounted and/or non-profit rates applicable to this Project." Should respondents provide a standard commercial rate alongside a separate non-profit rate, or submit a single non-profit rate schedule?
R: A comparison is preferred, but we will accept a single nonprofit rate schedule.

Q33. For CrowdStrike endpoint protection licensing — should respondents include this licensing cost in their proposal, or does the National Trust procure CrowdStrike independently?
R: Licensing should be included. We are currently getting this from our MSP.

Q34. For the eight geographically dispersed historic sites, does the National Trust require regularly scheduled on-site visits, or is a remote-first model with dispatch-based on-site support for hardware issues acceptable?
R: We handle the sites remotely and visit them once annually. This is typically done by NTHP internal IT.

Q35. Does the DC headquarters (Convene managed workspace) have any physical access restrictions or building management coordination requirements that would affect on-site IT support delivery?
R: There is very little equipment stored at Convene. Access is handled through our IT team (we would meet the vendor on site). We do need to request access to the server room. Currently, the only equipment on site is firewalls and two switches. Mac equipment is being decommissioned.

Q36. What is your budget range?
R: It is the policy of the National Trust not to release the budget during the RFP process.

Q37. Is NTHP using an centralized device management system (i.e. Intune, NinjaOne)?
R: We are implementing Intune right now for user endpoints. Server and firewall patching are done by MSP (for now).

Q38. Is a mobile device management platform being used manage BYOD mobile devices or organization-owned mobile devices? If so, what platform is used?
R: We are implementing Intune but do not plan to implement on personal devices (phones).

Q39. Are there any systems outside of the Azure environment needing backup? If so, how much data would need backed up?
R: We are talking about backing up our O365 environment. I am not sure of the amount of data to be backed up.

Q40. Does NTHP have a disaster recovery and business continuity plan or policy with defined recovery point and recovery time objectives? What technologies are being used for Disaster Recovery as a Service?
R: We get this as a service from the MSP.

Q41. What current Microsoft licensing is in use for users?
R: Business Premium, Business Basic, Visio, Intune

Q42. The RFP references both CrowdStrike and Microsoft Sentinel as components of the current cybersecurity stack. To better understand the existing security architecture and operational workflows, could you clarify how these platforms are being utilized together?

R: CrowdStrike handles primarily process behavior on servers and workstations while Sentinel handles Azure sign-ins and activity as well as network logging/alerting.

Q43. Which primary functions are assigned to CrowdStrike versus Microsoft Sentinel?
R: CrowdStrike handles primarily process behavior on servers and workstations while Sentinel handles Azure sign-ins and activity as well as network logging/alerting.

Q44. Is Sentinel being used primarily as the centralized SIEM/SOAR platform aggregating telemetry from CrowdStrike and other systems?
R: Sentinel and CrowdStrike are not integrated but validated alerts from both flow to ConnectWise.

Q45. Are there any overlapping detection, XDR, threat hunting, or incident response capabilities currently in use across both platforms?
R: Some threat intelligence overlaps between the two as we disseminate indicators.

Q46. Which platform serves as the primary system for alert triage, investigation, and response management?
R: Sentinel and CrowdStrike both.

Q47. Can the National Trust provide a sanitized current-state network topology and Azure architecture diagram showing the twelve managed locations, Azure environment, VPN connectivity, firewalls, switching, wireless infrastructure, and major cloud/security integrations?
R: We do not have this currently as our topology has changed in recent months.

Q48. The RFP states that the National Trust has one Azure subscription and that servers reside in Microsoft Azure with five hybrid servers. Can the National Trust provide a current Azure resource inventory, including virtual machines, storage, backup components, virtual networks, security services, and any production/development/test segmentation?
R: We are not sharing this currently.

Q49. Are Azure resources currently segmented by environment, business function, resource group, virtual network, or another model? If segmentation is not currently in place, should the selected MSP include recommendations as part of the roadmap?
R: We do not segment. There are no plans to add this to our roadmap.

Q50. What tools are currently used for endpoint management, patching, device compliance, and configuration enforcement across Windows and macOS endpoints?
R: Currently, ConnectWise is used by our MSP and we lease ConnectWise licenses from the MSP for our internal IT department. We are implementing Intune.

Q51. Are endpoints currently managed through Microsoft Intune, SCCM/MECM, JAMF, an incumbent MSP RMM tool, or another MDM/RMM platform? If incumbent-owned tools are currently in use, will those tools remain in place during transition or need to be replaced by the selected MSP?
R: MSP uses ConnectWise. This is through the MSP and will not remain in place after the transition.

Q52. What is the current patch compliance baseline for Windows endpoints, macOS endpoints, Azure servers, hybrid servers, SonicWall firewalls, switches, and wireless access points?

R: Monthly or as needed (critical patches get patched immediately).

Q53. How are SonicWall firewall policies, SSL VPN access, firmware updates, configuration backups, and rule changes currently managed across headquarters, regional offices, and historic sites?

R: VPN access is handled internally. Firewall policies are handled by MSP and NTHP. Backups handled through MSP (Veeam).

Q54. Are there any known recurring infrastructure issues, WAN performance concerns, VPN issues, wireless coverage issues, or network bottlenecks that vendors should account for in the proposal?

R: No

Q55. For Microsoft Sentinel and any other monitoring platforms currently in use, what log sources are integrated today, and what log retention requirements or expectations should vendors assume?

R: Sentinel is through the MSP.

Q56. How is identity and access management structured across Microsoft Entra ID/Azure AD, Okta, and Office 365? Please clarify which platform is authoritative for authentication, MFA, SSO, lifecycle management, and privileged access.

R: AD is the source of truth. From AD, data syncs to Okta.

Q57. Are MFA and Conditional Access policies fully implemented for all users, administrators, service accounts, and privileged accounts? If not, should the selected MSP include assessment and remediation recommendations?

R: Yes, MFA is fully implemented.

Q58. The RFP lists CrowdStrike, Defender, Sentinel, Okta, Veeam backups, and DRaaS as part of the current environment. Which of these tools are licensed or procured by the National Trust versus provided through the incumbent MSP, and which are expected to remain in place after transition?

R: NTHP handles the licensing for Okta and Defender. Crowdstrike, Sentinel, Veeam and DRaaS is procured through our current MSP.

Q59. What CrowdStrike and Microsoft Defender capabilities are currently active today, including EDR, alerting, endpoint isolation, threat hunting, automated remediation, vulnerability visibility, and managed response?

R: Monitoring, alerting, isolation, etc. is handled by MSP. A fully developed SOC is a requirement of this RFP.

Q60. How are security alerts currently triaged, escalated, documented, and remediated between internal IT staff, the incumbent MSP, and any SOC resources?

R: MSP contacts the VP of Information Technology or lead Network Administrator of any security incidents. If there is a security issue, MSP has permission to lock down the impacted account/application. Servers are set up for monitoring and the internal IT team is alerted via email if there is a server, switch or WAP offline. Security incidents are logged and written explanations of incidents are sent to the VP of IT.

Q61. How frequently are vulnerability scans performed today, what tools are used, and what is the current process for remediation ownership, patch validation, and executive reporting?

R: Annually

Q62. Are annual penetration tests, third-party security assessments, or cyber risk assessments currently performed? If yes, should vendors assume responsibility for coordinating or supporting these activities under the MSP scope?

R: We do not do annual penetration tests. We have had a third party assessment done in the past to identify any risks.

Q63. What backup retention, recovery point objective, recovery time objective, and DR testing requirements should vendors assume for Azure servers, hybrid servers, endpoints, SharePoint, and other critical systems?

R: Recovery Time Objective – (4) hours
Recovery Point Objective – (8) business hours
One annual disaster recovery test and up to 3 automated Disaster recovery tests.

Q64. How is Veeam currently integrated into the Azure and hybrid infrastructure, and is the existing Veeam environment owned/licensed by the National Trust or the incumbent MSP?

R: Veeam backs up all data files and servers multiple times per day. Veeam is licensed by MSP. Note, backups are not part of this RFP as we are under contract until May 2027 with incumbent MSP.

Q65. What centralized asset inventory, configuration management, documentation, credential management, and secrets management platforms are currently in place?

R: Asset inventory is managed through ConnectWise and Monday.com.

Q66. Are there any unsupported operating systems, legacy hardware, end-of-life network devices, or technical debt items currently in production that vendors should include in transition and roadmap planning?

R: There are no unsupported operating systems, legacy hardware or technical debt items.

Q67. What integrations currently exist between Microsoft 365, SharePoint, Okta, Sentinel, CrowdStrike, Defender, Veeam, and any third-party operational or monitoring tools?

R: AD and Entra ID are the base. Okta, Sharepoint, etc. use AD/Entra ID credentials. CrowdStrike is pushed and Veeam is used for server backups.

Q68. How are production changes currently requested, approved, documented, and communicated between the National Trust IT team and the current MSP?

R: Changes are requested by the VP of Information Technology to MSP via email. Tickets are created to manage the progress of the request.

Q69. What documentation will be made available during onboarding, including network diagrams, Azure documentation, firewall configurations, backup/DR documentation, asset inventories, administrative procedures, vendor contacts, licensing details, runbooks, and historical ticket data?

R: The following will be shared during onboarding – Azure documentation, Network documentation, licensing details.

Q70. Can the National Trust provide guidance on whether vendors should propose a baseline/core services model with optional add-on services for the budget range?

R: We are not providing a set budget range. Your quote should include the items listed in the RFP, but you can list 'add on' services not requested in the RFP.

Q71. Should vendors structure pricing as one consolidated monthly recurring service fee, or does the National Trust prefer pricing separated by service category, such as infrastructure management, cybersecurity/SOC services, endpoint protection, Azure management, backup/DR, consulting, onsite support, and transition/onboarding?

R: One consolidated monthly recurring fee. Please itemize what the monthly fee includes.

Q72. Should one-time transition, onboarding, documentation review, and incumbent MSP knowledge-transfer costs be priced separately from recurring monthly managed services?

R: Please include one-time transition costs if it is not included as part of the main contract.

Q73. Should vendors provide pricing for the full three-year term with fixed annual pricing, or may vendors include annual escalation assumptions?

R: We plan to do a multi-year agreement. If there is an annual escalation, please provide what your organization's escalation schedule.

Q74. Will the National Trust allow vendors to provide multiple pricing options, such as a base MSP package with optional cybersecurity, DR testing, onsite support, and project consulting enhancements?

R: Your reply should include a monthly recurring fee for the items listed in the RFP. Additional add-on pricing can be submitted.

Q75. The RFP asks vendors to identify whether service desks and engineers are onshore, offshore, or hybrid. Will the National Trust consider a hybrid delivery model that includes U.S.-based leadership and escalation with nearshore technical resources aligned to U.S. time zones?

R: Engineers must be in the United States. Since we only utilize service desk for Tier 3 escalation, nearshore technical resources could be considered but are not preferred.

Q76. Are there any restrictions or preferences related to offshore, nearshore, or non-U.S.-based technical resources for infrastructure support, cybersecurity monitoring, endpoint management, Azure administration, or after-hours support?

R: Main technical contacts must not be offshore/nearshore, or non- US based resources. Would consider near-shore cybersecurity monitoring.

Q77. For onsite support, should vendors assume work will be performed remotely unless scheduled onsite support is required, or does the National Trust expect recurring onsite presence at headquarters, regional offices, or historic sites?

R: Vendors should assume that most work will be performed remotely.

Q78. If onsite support is required, should travel and related expenses be included in the fixed managed services pricing, or priced separately as needed?

R: Travel should be priced separately as needed.

Q79. Is the current MSP's delivery model entirely local, or are any services currently delivered through regional, national, global, subcontracted, offshore, or nearshore resources?

R: The current MSP's delivery model is delivered regionally and nationally. They do not subcontract work.

Q80. Will the incumbent MSP be required to participate in a formal transition and knowledge-transfer process? If yes, what overlap period should vendors assume for onboarding, access transfer, documentation transfer, and tool/license transition?

R: If we should go with a new vendor, the incumbent MSP will participate in a 30-day knowledge transfer process.

Q81. What level of transition support and knowledge transfer is expected from the incumbent MSP during onboarding, and is there an anticipated overlap period between providers?

R: We anticipate an overlap period of one month.

Q82. What are the expected support hours for Tier 2/Tier 3 infrastructure support? Is after-hours, weekend, or holiday support expected beyond cybersecurity SOC monitoring requirements?

R: No. Our internal IT department handles after-hours, weekend and holiday support. However, in the event of an emergency, we do have resources with the incumbent that we can contact.

Q83. Are there any cybersecurity frameworks, regulatory obligations, cyber insurance requirements, or security standards (e.g., NIST CSF, CIS Controls, SOC 2 alignment, nonprofit grant-related compliance) that the MSP must support or align with?

R: SOC 2 alignment

Q84. Can the National Trust provide expected SLA requirements for response and resolution times by incident severity, escalation expectations, and uptime/availability targets?

R: SLA Matrix –

- **Critical (system down) response within 1 hour.**
- **High – response within 2 hours; resolution within 8 hours**
- **Medium – response within 4 hours**
- **Low – Response within 8 hours**

Q85. What are the National Trust's top strategic IT priorities over the next 3–5 years (e.g., Azure modernization, zero trust, M365 optimization, macOS expansion, security maturity, automation, cost optimization)?

R: Security maturity, AI adoption, cost optimization.

Q86. Should respondents assume large infrastructure/security projects (e.g., network refreshes, migrations, major cybersecurity initiatives) are expected to be included within the managed services fee, or quoted separately on a time-and-materials/project basis?

R: Currently, large projects are quoted separately than the monthly managed services fee. Please discuss your preferred method.

Q87. Does the National Trust have any preferred subcontracting, MWBE, small business, disadvantaged business, or diversity participation goals or targets for this contract? If so, are there minimum percentages or reporting requirements?

R: No

Q88. Are there any anticipated organizational, infrastructure, application, or staffing changes (new locations, acquisitions, endpoint expansion, Azure growth, macOS

expansion, historic site technology upgrades, etc.) expected during the contract period that respondents should account for in pricing and staffing assumptions?

R: Possible Mac expansion. There could be historic site technology upgrades (as our budget allows), but this mainly includes cabling, wireless access across large campuses, and the adoption of virtual reality applications for tours and exhibits.

Q89. What level of existing documentation is currently available (network diagrams, asset inventory, SOPs, credential management, runbooks), and are there known gaps respondents should anticipate during onboarding?

R: Network diagrams are being updated due to our recent migrations to Microsoft Azure. We will share credential management and SOP's.

Q90. Beyond monthly and quarterly reporting, what KPIs or success metrics will the National Trust use to evaluate MSP performance during the contract term (e.g., MTTR, vulnerability remediation timelines, ticket resolution, uptime, user satisfaction, security posture improvements)?

R: KPI's will be measured by user satisfaction (mainly, IT being satisfied with progress on projects, issue resolution and security improvements.

Q91. Could you please provide detailed information about your infrastructure, including the number of routers, switches, access points, firewalls, servers, etc.?

R: Sonic Wall Firewalls TZ370(11), TZ270 (1), NSA2700 (2),
Azure-NSv470 (1)
Meraki Switches 12
Meraki Access Points 65
Hybrid Servers (Azure) 5

Q92. How many employees do you currently have?

R: 240 full time/150 seasonal part time

Q93. Do you require onsite support or open for Hybrid model?

R: Support is done remotely. Project work at sites could require onsite resources.

Q94. We would like to clarify whether you are seeking a one-time project engagement or ongoing monthly support services as well.

R: Ongoing monthly support as stated in the RFP.

Q95. Can you please explain connectivity from enterprise network to Azure as it exists today?

R: Site to Site VPN

Q96. Is the SSL VPN SonicWALL, and if so does it operate as a separate physical box?

R: The SSL VPN is Sonicwall. It does not operate as a separate physical box.

Q97. Are any firewalls in azure as VMs?

R: Yes. Azure-NSv470

Q98. How many firewalls total across the enterprise? Do they have support contracts? Provide all models.

R: Sonic Wall Firewalls TZ370(11), TZ270 (1), NSA2700 (2),
Azure-NSv470 (1)

Q99. Please provide all models and full counts for Meraki switches and AP. Are they all in one Meraki portal or separate? How many SSIDs? Do you use NAC? When does the licensing expire?

R:

Meraki Switches 12
Meraki Access Points 65
Hybrid Servers (Azure) 6
Licensing renews annually.
Approximately 30 SSID's (includes guest networks).

Q100. Please provide all models of Aruba Switches. Provide license, support info, and code versions.

R: We only have two Aruba switches. These devices are not overly relevant to this RFP.

Q101. Please provide all models of Dell Switches. Provide license, support info, and code versions.

R: We use Meraki Switches.

Q102. We understand the network infrastructure consists of Dell, Aruba, Meraki, and SonicWALL. Is there a plan to consolidate this infrastructure to a single or fewer vendors? Is NTHP open to this approach?

R: Dell switches are currently being replaced by Meraki switches. There are only two Aruba switches in our infrastructure. These will be switched when they are EOL.

Q103. For EDR, does NTHP expect the awardee to manage the existing EDR solution or provide an EDR solution as a service?

R: EDR as a service.

Q104. Does the awardee need to scope both a replacement service and a project to migrate for all the following services? CrowdStrike, Sentinel, Defender, Veeam Backups.

R: CrowdStrike, Sentinel and Veeam are leased through the MSP. We assume that we would go with the security stack that a new MSP uses.

Q105. Are any of these platform licenses transferable?

R: No

Q106. For any new service provided by the awardee, does NTHP require the awardee to own the license (as a service) or is it desired that NTHP own the service to be managed by the awardee?

R: We desire that the MSP owns the license.

Q107. Azure Subscription Questions:

- How do you manage lifecycle operations for Azure VMs?
- Does your current MSP own the subscription?
- What monitoring platform(s) do you use?
- What metrics are monitored for Azure VMs?
- Describe your patch management process for Windows VMs?
- What is your standard patching schedule?
- What vulnerability scanning tools do you use?
- What backup technologies do you use outside of Veeam?
- How do you track and report Azure spend? Would FinOps reporting be a requirement?

- Provide your standard SLA matrix.

R:

- **Current MSP does not own the subscription.**
- **Patch management is handled by MSP**
- **Patch management is monthly (sooner if a critical vulnerability is released).**
- **Backup Technologies – Azure and Veeam**
- **We manually track Azure spend.**
- **SLA Matrix –**
  - **Critical (system down) response within 1 hour.**
  - **High – response within 2 hours; resolution within 8 hours**
  - **Medium – response within 4 hours**
  - **Low – Response within 8 hours**

Q108. 0365 Tenant Questions

- Describe your Entra ID (Azure AD) management capabilities.
- How many total users or mailboxes?
- Are there any shared mailboxes?
- Describe your Entra ID (Azure AD) management capabilities.
- Do you use SharePoint online and One-Drive?
- Describe your Microsoft 365 security management framework
- Do you use End-point Management via Intune?
- What Microsoft 365 backup solutions are currently being leveraged?
- What is the retention policy and RTO associated?

R: The VP of IT and Network Admin has full management capabilities along with our MSP.

- **Approximately 390 users (240 are full time staff/150 seasonal employees with limited technology offerings (email, ADP, Okta)**
- **We use SharePoint and One Drive**
- **We are currently implementing Intune.**

Q109. End Points – Windows 300 and mac 5 Questions

- Describe your endpoint provisioning process.
- What tools are currently being utilized for endpoint deployment?
- For Mac do you use Apple Business Manager? Or any third-party tool?
- Describe your patch management process.
- How frequently are patches deployed?
- Describe your third-party software update approach
- Describe your endpoint security management?
- Describe your ransomware protection capabilities.
- How are security incidents detected and escalated?
- Are MFA, Conditional Access and SSO currently being configured?
- Any compliance and Governance to keep in mind? (HIPPA, SOC2, ISO 27001, PCI, DSS)
- How is HW, SW inventory along with warranty information being maintained?
- Are systems running Windows 10/11?
- Is BitLocker Enabled on endpoints?

R: Computer builds are handled by internal IT staff.
Endpoint patching is handled monthly by MSP.
Endpoint security patching is currently handled by MSP, but we are implementing Intune. I am not sure if we will fully manage updates or if MSP will use our Intune account to do so.
All security monitoring is handled by MSP.

Third party endpoint updates are handled by internal NTHP staff using Ninite. HW and SW inventory handled in Monday.com.

Q110. What services are expected to remain with internal IT vs. MSP, especially since help desk and application support are handled internally?

R:

- **NTHP Responsibility**
  - **Help Desk (escalation on Tier 3 items when internal team can't resolve)**
  - **Procurement and lifecycle management of devices**
  - **Application management**
  - **Okta**
  - **SSL renewal and DNS management**
  - **SharePoint administration**
  - **Endpoint patching**
- **MSP**
  - **Server/Switch/access point patching**
  - **SOC Services (24x7x365 system monitoring),intrusion and malware analysis, threat intelligence, incident response and remediation**
  - **Firewall patching**
  - **High level consulting**
  - **Security hardening**

Q111. Should MSP provide Level 1 support backup, or strictly Tier 2/3 as defined?

R: MSP will only provide Tier 2/3 support.

Q112. Are there any services currently delivered by the incumbent MSP that are NOT required moving forward?

R: No

Q113. Are MSPs expected to manage all infrastructure components (network, servers, cloud, endpoints) or only specific layers?

R: All infrastructure components

Q114. Are there any non-Azure/on-prem legacy systems not mentioned in the RFP?

R: No

Q115. What is the current network topology across the 12 locations?

R: All locations main setup is as follows:
ISP router, SonicWALL Firewall, Meraki switches connecting to wireless access points. Some sites have multiple buildings connected to the network along with outdoor Meraki WAPs.

Q116. Are there any planned infrastructure changes or expansions (e.g., Mac environment growth)?

R: We could possibly expand our Mac environment.

Q117. What is the exact endpoint count by type (laptops/desktops/servers/mac devices)?

R: Macs – 6, Laptops 295, desktops 15, servers (5 hybrid servers in Azure, 9 remote locations fully in Azure.

Q118. Are endpoints currently managed via Intune or another MDM tool?

R: We are implementing Intune

Q119. Are MSPs expected to support procurement/lifecycle management or only management of existing devices?

R: Procurement/lifecycle management is handled by the internal team.

Q120. Which tools (CrowdStrike, Sentinel, Defender, etc.) are mandatory vs. replaceable by MSP?
R: Comparable tools could be used.

Q121. Should the MSP provide SOC using existing tools or propose its own stack?
R: MSP provides their own stack. Our current stack is through our incumbent MSP.

Q122. Who owns identity management (Okta) responsibilities long-term?
R: This is managed internally. Incumbent MSP assists with configurations/integrations with Oka when implementing new technologies (such as Intune).

Q123. What are the required support hours (24x7 vs business hours)?
R: – Systems and cyber should be monitored 24x7. Internal support is handled by NTHP internal IT staff.

Q124. Are MSPs responsible for license management or only technical operations?
R: It depends on the license. Example – Office 365 is managed internally by NTHP IT staff. Anti-virus handled through MSP.

Q125. What are the current RPO/RTO requirements?
R: We need to be able to restore to the previous business day.

Q126. Should MSP manage Veeam and DRaaS fully, or only monitor?
R: Veeam and DRaaS is currently handled by the MSP. This is managed fully by MSP. This is not part of the current RFP as we are under contract for DRaaS through May 2027.

Q127. Are there any BCP/DR testing requirements or schedules?
R: We would like to do this, but there is none scheduled at this time.

Q128. What level of on-site support is required across locations?
R: None. This is managed by internal IT staff. There could be instances during the duration of the contract where we may need onsite assistance for project work, but that would be handled under a separate contract.

Q129. Are there existing vendor contracts (ISP, hardware support) the MSP must coordinate with?
R: No. This is handled by Internal IT staff.

Q130. Are network upgrades/standardization initiatives planned?
R: We are just completing migrations to Azure. No additional upgrades planned at this time.

Q131. Should MSP include RMM, SOC, and security tools in pricing, or use existing tools?
R: Include this in pricing. Existing tools for RMM and SOC are owned by incumbent MSP.

Q132. Are there restrictions on offshore or hybrid delivery models?
R: We do not want offshore support (see RFP).

Q133. Is there a requirement for dedicated resources vs shared pool?

R: We would like one dedicated resource (see RFP), but shared resources for technical expertise is desired.

Q134. Do you expect an onsite presence (regular/periodic)?
R: No