

A) Goals, Fit, and Division of Responsibilities

1. What are the top 3 outcomes NCCDI wants from the selected provider in the first 90 days?

We would like to see our Active Directory environment fully transitioned to the cloud and decommission as many of our physical servers as possible. We would also like to discuss and set up an MDM solution for our Apple iPads and Google Chromebooks (preferably integrated with Intune).

2. What are the biggest IT pain points today (response time, recurring issues, onsite delays, reporting, security concerns, etc.)?

We have three IT pain points:

1. We don't have the manpower to tackle bigger projects. When we do pull our focus from day-to-day operations to bigger projects, we get behind in the daily tasks.
 2. Lack of staff training on using Microsoft 365, identifying scams and phishing schemes, etc.
 3. Lack of response time/initiative from 3rd party IT.
3. How do you envision the work being divided between the in-house IT Specialist and the selected vendor (help desk vs tier 2/3 escalation vs projects vs strategic IT management/(v)CIO support)?

Vendor handles out-of-business hours support and monitors servers, and consults based on request from in-house IT. Vendor also supplies and monitors antivirus.

B) Support Demand and Coverage Expectations (Pricing Drivers)

4. What has your average monthly ticket volume been over the last 6–12 months (and any seasonal peaks)?

Our average ticket volume is 11-15 per month, not including phone calls, emails and in-person contact. Estimate including non-ticket contact would be about double, 22-30/month. Seasonal peaks include August and January when staff are coming back from large breaks.

5. What support coverage is expected (business hours only vs after-hours/on call for critical events)?

Mostly after-hours, with business hours as needed for consults with in-house IT.

6. Do you have preferred response and resolution targets by severity level (e.g., critical outage vs standard request)?

Yes, although critical outages would be rare.

7. Roughly how often is onsite support required at each location (monthly estimate)?

None from 3rd-party IT.

C) Locations, Connectivity, and Network Management

8. How are the eight sites connected today (MPLS (Multi-Protocol Label Switching), site-to-site VPN, SD-WAN, mixed)?

We have a mixed WAN, utilizing an MPLS circuit, and site-to-site VPNs through our firewalls.

9. Who currently manages internet circuits, firewalls, and wireless infrastructure (internal, current vendor, ISP-managed)?

Both the ISP and our current 3rd-party IT vendor.

10. Are there known chronic issues at specific sites (internet instability, Wi-Fi coverage gaps, VPN drops, etc.)?

Lotus Center (10 Damon Avenue, Red Bluff, CA) has inconsistent internet connectivity—this is most likely a hardware fault of the ISP.

D) Infrastructure and Remote Access (Servers/VMware/Azure/Remote Desktop)

11. For the on-prem servers and the Azure-hosted components, can you confirm server roles and the high-level architecture (e.g., Active Directory (AD), file/print, Remote Desktop Services (RDS), application servers; VMware version and host environment)?

We are currently running in a hybrid environment, with Active Directory syncing to Entra and making use of 365 groups and 365 for SharePoint and Exchange services. We also use OneDrive for file storage as opposed to any local sync alternatives. We are looking to fully decommission our AD DCs and move to Entra only.

12. Do you currently use Remote Desktop Services (RDS) and/or thin clients? If yes: approximately how many users and where is it hosted?

No.

13. Are there any known or planned initiatives during the 36-month term (site expansion, server/firewall refresh, Microsoft 365/identity/security initiatives) you already anticipate vendor involvement in?

We would like our vendor to help us fully decommission our local servers and transition us fully to cloud-based architecture. We would like to upgrade our firewalls to have at least a 2.5GbE throughput and transfer our Access Control Lists etc. to the updated version of SonicOS as well as removing our site-to-site VPNs, as we no longer have need for a WAN.

E) Microsoft Identity and Licensing (Entra Hybrid / Microsoft 365)

14. Can you confirm the identity setup (on-prem AD + Entra sync) and whether Multi-Factor Authentication (MFA) / Conditional Access is currently enforced?

Yes, we have a hybrid on-prem/Entra sync environment, and MFA is enforced for most users. We have Conditional Access rules, however they are not as strict as they could be.

15. Does NCCDI want the vendor to manage Microsoft nonprofit licensing optimization and ongoing administration, or remain internal?

We will manage the amount of licenses, but we would like the vendor's assistance in seeking a nonprofit discount if applicable.

F) Security Expectations

16. You mention SentinelOne and Webroot—are both currently deployed, and if so, how are responsibilities divided (coverage, alerting, response)?

S1 and Webroot are both deployed on every endpoint, though threat response is mitigated through S1 exclusively. We would like to trim down to only one antivirus solution if possible, and would like to move away from S1 as it has caused multiple ongoing software issues both in the past and currently.

17. Do you have standards you want enforced for endpoint encryption (BitLocker/FileVault), device compliance, or security training/phishing simulation?

We would like to continue our phishing simulation services and would like to enforce BitLocker on all devices. BitLocker is currently enabled through our MDM (Intune), but a stricter implementation would be welcome as long as recovery keys are easily accessible.

18. Have there been any security incidents in the last 24 months that should inform the selected provider's initial priorities? (Even high-level details are helpful.)

We have luckily not experienced many security incidents in the past 24 months. The largest have been a botnet attack on our local firewall login which was mitigated by changing the access port, and attempts to log in to staff 365 accounts which was mitigated by enabling 2FA.

G) Backup / Disaster Recovery (BDR + Cloud Replication)

19. What backup and disaster recovery (BDR) platform is currently in place, and what are your retention and replication expectations?

We have no BDR solution currently. We previously had one with our on-prem solution, though we are searching for one as we transition to the cloud.

20. When was the last successful restore test performed (file restore and full VM/server restore)?

Approximately one year ago.

21. Do you want the vendor to own and document periodic DR testing and provide regular backup/DR reporting?

Because of the nature of our environment, we don't believe that Disaster Recovery services are going to be as valuable, so that is not currently a priority of ours.

H) Applications and Vendor Boundaries

22. For Child Plus, ADP Workforce Now (ADP WFN), and Blackbaud Financial Edge: where do you want the vendor's responsibility to begin/end vs the application vendor?

We would like to leave LoB and app vendor responsibilities to their respective department heads; we do not host any local data for those services.

23. Are there other critical systems not listed (VoIP, cameras / Network Video Recorder (NVR), door access control, managed print, etc.) that should be included in scope?

No.

I) Commercial Terms (So We Price Correctly)

24. For multi-site onsite support, should travel time/mileage be included in the monthly fee or billed separately? If separately, what rules do you prefer?

Billed separately. We follow federal rules regarding mileage reimbursement.

25. Reliable Technology Solutions typically provides managed services under a monthly plan, with projects/out-of-scope billed separately. Does NCCDI prefer project work quoted fixed-fee when possible, time-and-materials, or depending on the project?

We would prefer billing to depend on the project.