National Children’s Alliance

Co-Managed IT Services — Consolidated Questions & Answers

RFP No. NCA-IT-2026-01 • Posted July 22, 2026

The following consolidated questions and answers respond to inquiries received from prospective respondents through the question deadline of July 17, 2026. In accordance with Section 11 of the RFP, these responses are shared with all known respondents. Questions have been consolidated and, where similar, combined, and may be lightly edited for clarity. The RFP (No. NCA-IT-2026-01) remains the sole controlling document; where a response and the RFP appear to differ, the RFP governs as amended by these answers.

Microsoft 365 Licensing & Configuration

Q1. Will NCA continue to procure and own all Microsoft licensing directly, with the provider administering those services, or should respondents include Microsoft licensing costs? If customer-owned, can a licensing summary by SKU and quantity be provided?

NCA will continue to procure and own its existing Microsoft 365 licensing directly. Respondents should exclude existing Microsoft licensing from their core service pricing and identify any recommended additional licenses separately. A full current licensing summary will be provided to the selected vendor during onboarding.

Q2. Have Intune, Defender, Purview, Conditional Access, Windows Autopilot, and Entra ID been implemented to the desired level, or should respondents anticipate significant implementation and remediation during onboarding?

NCA has already implemented Microsoft Entra ID, MFA, Conditional Access, Intune, Windows Autopilot, Microsoft Defender, and Microsoft Purview; respondents should not assume a greenfield implementation. All active NCA-issued Windows laptops are managed through Intune, and 50 devices are registered in Windows Autopilot (one recent compliance-policy report showed 60 of 63 evaluated devices compliant). The Section 4.1 onboarding phase is expected to include an assessment followed by targeted cleanup, remediation, hardening, and standardization — including stale or duplicate device records, policy errors, policies in report-only or simulation mode, vulnerability findings, patching, and documentation.

Q3. Should respondents assume NIST SP 800-171 Revision 2 or Revision 3?

Respondents should use **NIST SP 800-171 Revision 3** as the current reference baseline. NCA is seeking appropriate framework alignment for its environment and federal-grantee responsibilities, not representing that it currently holds a formal certification under the standard.

Tooling, Security & Assurance

Q4. Can NCA provide a list of current security and management tools (RMM, MDR, SIEM, M365 backup, vulnerability management, documentation, ticketing) to help respondents avoid redundant solutions?

NCA operates a Microsoft-centric environment: Microsoft Entra ID, MFA, and Conditional Access; Microsoft Intune and Windows Autopilot; Microsoft Defender for endpoint, email, exposure, and vulnerability management; Microsoft Purview DLP and retention; an existing Backupify application; and internal Microsoft 365-based support intake and documentation. NCA does not currently use an MSP RMM or PSA platform, an external 24/7 MDR/SOC service, or a separate third-party SIEM. Per Section 4.2, respondents must describe how they will use and integrate with this existing Microsoft stack before proposing additional tooling; any additional tools must be justified and priced separately.

Q5. Does NCA currently use a third-party Microsoft 365 backup solution, and should respondents assume it remains or propose an alternative?

A Backupify integration is present in the tenant; NCA is validating its current subscription status, protected workloads, retention settings, and restore history. Respondents should assess the existing solution and may propose an alternative, priced separately, consistent with Section 4.8.

Q6. Has NCA recently completed any security assessments, penetration tests, Microsoft Secure Score reviews, or NIST/CIS gap assessments that will be available to the selected vendor?

NCA has not identified a recent formal penetration test, NIST/CIS gap assessment, or documented Secure Score review available for distribution. Current Microsoft security and compliance reporting can be shared during onboarding, and respondents should assume the Section 4.1 phase will include a current security baseline and gap assessment.

Q7. Would NCA accept a combined assurance package (applicable data-center and critical-service-provider SOC reports and bridge letters, together with the respondent's internal-control, access-governance, personnel-screening, risk-management, insurance, and framework-alignment documentation) as the "equivalent" permitted by the RFP?

NCA will consider a combined assurance package as a potential equivalent to a SOC 2 Type II report but cannot confirm acceptance in advance. Respondents proposing an equivalent should include the complete package with their proposal — applicable SOC reports and bridge letters, the controls and reporting periods covered, independently assessed components, and any identified exceptions or gaps. NCA will evaluate whether the package adequately addresses the applicable security, privacy, contractual, federal-grant, and data-protection requirements, and may request additional documentation during evaluation.

Support & Operations

Q8. What is NCA's average monthly service desk ticket volume, and how are tickets divided between Tier 1, Tier 2, and Tier 3?

Based on internal tracking over approximately the past three and a half months, NCA averages about **25 in-scope service requests per month**. NCA has not historically categorized requests by tier; the following is an estimate. Tier 1 (~60–65%): password and account assistance, MFA re-registration, routine how-to questions, basic application support, account setup, and approved access changes. Tier 2 (~25–30%):

device and application troubleshooting, SharePoint/OneDrive issues, Adobe/Microsoft 365 application problems, and Intune-related troubleshooting. Tier 3 (~5–10%): more complex endpoint, identity, security, or multi-system troubleshooting within scope. Retained internal responsibilities, strategic projects, and out-of-scope systems are not included.

Q9. Approximately how many after-hours or weekend support requests and security incidents does NCA experience in a typical year?

NCA does not currently track after-hours volume separately. Based on recent experience, after-hours or weekend support requests and security incidents are rare — generally only a few per year. NCA still expects 24/7 response capability for critical security incidents and business-down events.

Q10. Which Microsoft 365 administrative responsibilities remain with internal staff versus the selected co-managed partner?

NCA's internal IT lead retains responsibility for organization-specific context, approvals, priorities, access governance, identity ownership, vendor relationships, and certain routine administrative work. The selected partner provides Tier 1–3 end-user support, advanced escalation, Intune administration at scale, patch and vulnerability management, 24/7 security monitoring and response, Microsoft 365 backup, hardware lifecycle support, and maintained documentation. Microsoft 365 and Entra administration, onboarding/offboarding automation, security policy, incident response, license optimization, and technology planning are shared responsibilities.

Q11. Is NCA currently working with an MSP or other IT provider, and will the selected vendor receive a transition period and cooperation from the incumbent?

NCA does not currently engage an external co-managed IT provider for the services covered by this RFP; these services have been handled internally. There is no incumbent provider to transition from. The selected vendor will work directly with NCA's internal IT lead, and onboarding will begin with the discovery and baseline process in Section 4.1 using NCA's existing documentation and inventory.

Azure Environment

Q12. Should respondents assume responsibility for any identity, networking, authentication, or security dependencies between the Microsoft 365 environment and the out-of-scope Azure resources, or are those entirely managed by the existing Azure provider?

The Azure-hosted REDCap/MySQL resources, VPN/VNet, database, and associated application infrastructure are outside the scope of this engagement and are managed separately. The selected partner should support Microsoft 365 and Entra-side identity, authentication, and security dependencies within its scope. Any work requiring changes to the Azure infrastructure should be coordinated through NCA's internal IT lead and the parties responsible for that environment.

Hardware

Q13. Approximately what percentage of the Dell laptop refresh is complete, and how many devices remain to be deployed?

NCA's fleet refresh to Dell Pro / Pro Max 16 laptops is substantially underway, with new units already deployed under active manufacturer ProSupport coverage held by NCA and a small number of devices remaining to be deployed. Exact figures are being finalized from asset and purchasing records and can be shared with the selected vendor during onboarding.

Q14. How many laptops are enrolled in Intune and Windows Autopilot, and approximately how many new deployments, returns, departures, and warranty cases occur annually?

NCA maintains approximately 50 active organization-owned Windows laptops, all enrolled and managed through Microsoft Intune. Intune currently contains 73 Windows device records (including older devices, spares, and duplicates still present in the environment); 50 devices are registered in Windows Autopilot. Approximate annual activity: new device deployments 6–10; warranty or hardware-replacement cases 5–10; employee departures and device returns 5–8. These are planning estimates and may vary.

Q15. Does NCA anticipate procuring hardware directly through nonprofit purchasing programs, or should respondents expect to procure hardware on NCA's behalf?

Per Section 4.9, respondents should price **both** (a) a provisioning-only model, in which NCA procures hardware directly (including through nonprofit purchasing programs) and the partner configures and enrolls it, and (b) full procurement with markup. NCA will determine its preferred approach during evaluation.

Federal Procurement & Contracting

Q16. Is an active SAM.gov registration required at proposal submission, or only before contract award?

An active SAM.gov registration with a valid Unique Entity ID is required prior to contract award. Respondents need not have completed registration at proposal submission but should be registered or actively in process. Attachment A (field 1.13) and the Section 11.3 submission list are amended accordingly: respondents whose registration is pending should indicate their registration status in lieu of a Unique Entity ID at submission.

Q17. Will NCA accept a pending SAM.gov registration if the respondent provides evidence that registration is in process?

Yes. NCA will accept a proposal from a respondent whose SAM.gov registration is pending, provided evidence that registration is in process; active registration remains a condition of award.

Q18. Will NCA provide the specific 2 CFR Part 200, Appendix II provisions to be incorporated into the final agreement, or should respondents include their own proposed federal flow-down language?

NCA will provide the applicable 2 CFR Part 200, Appendix II provisions for incorporation into the final agreement; respondents need not draft their own federal flow-down language. Respondents should note in their proposal any Appendix II provision they are unable to accept.

Q19. Are there specific invoice formats, labor categories, cost allocations, or supporting documentation NCA requires to demonstrate cost reasonableness and allowability?

NCA requires itemized invoicing consistent with the pricing structure in Section 10, sufficient to support cost reasonableness and allowability under 2 CFR Part 200, with pass-through and tooling costs identified. NCA does not mandate a specific invoice template but reserves the right to request a cost or price breakdown.

Q20. For the three-year record-retention requirement, does NCA expect access only to records related to this engagement, or to broader company financial records?

The retention and access requirement applies to service and billing records related to this engagement (consistent with 2 CFR 200.334), not to the respondent's broader company financial records.

Q21. Would any inspection or audit of service and billing records be subject to reasonable confidentiality and data-security protections?

Yes. Any inspection or audit of records will be subject to reasonable confidentiality and data-security protections, consistent with the confidentiality terms in Section 8.

Q22. Does NCA require a formal conflict-of-interest disclosure with the proposal, even when no conflict or prior relationship exists?

Yes. NCA requests a conflict-of-interest disclosure with every proposal, including an affirmative statement where no conflict or prior relationship exists.

Q23. Are subcontractors and third-party technology providers (MDR, backup, security-awareness, software vendors) subject to the same SAM.gov and debarment requirements?

The selected partner must ensure that any subcontractor performing work under this engagement in a covered transaction of $25,000 or more is not suspended, debarred, or otherwise excluded (verified via the SAM.gov exclusions system). Full SAM.gov registration is required of the prime contractor; it is not required of every commercial software or tooling provider.

Q24. Does NCA anticipate any additional federal agency-specific terms, beyond those listed in the RFP, applying to the engagement?

These services are funded as an indirect cost across NCA's federal award portfolio (primarily U.S. Department of Justice / OJJDP). The applicable requirements are the Uniform Guidance (2 CFR Part 200) and DOJ Financial Guide provisions referenced in the RFP. NCA does not anticipate additional agency-specific flow-downs beyond those but reserves the right to incorporate any that apply at award.