National Children's Alliance

Co-Managed IT Services — Consolidated Questions & Answers

RFP No. NCA-IT-2026-02 • Posted September 14, 2026

These consolidated questions and answers respond to inquiries received from prospective respondents through the September 9 question deadline. In accordance with Section 11, they are shared with all known respondents, consolidated and lightly edited for clarity, and not attributed to individual firms. The RFP (No. NCA-IT-2026-02) remains the controlling document; where a response and the RFP differ, the RFP governs as amended by these answers. NCA is an established, actively managed environment; detailed current-state information will be provided to the selected vendor under NDA during the Section 4.1 discovery and baseline phase. All further questions must be submitted in writing to jread@nca-online.org.

Clarification to Section 2 — Microsoft Licensing

NCA's core licensing is **Microsoft 365 Business Premium** under Microsoft's nonprofit program, with select add-on licenses for specific functions (e.g., Copilot, Teams Phone). References to "E5-level" in Section 2 should be read accordingly. Respondents should scope and price against current (Business Premium) licensing. Proposed licensing changes or upgrades may be presented as separately priced options consistent with Section 4.14. All Microsoft licenses are organization-owned.

Support Model & U.S.-Based Support (Section 5.10)

Q. How does the U.S.-based support requirement apply — including nearshore Tier 1, offshore MDR monitoring, or a subcontracted SOC?

All levels of support that access NCA systems or data — including the Tier 1 service desk — must be performed by personnel located within the United States. Tier 1 work involves access to NCA systems and user accounts by nature, so it falls inside the requirement. A U.S.-based subcontracted SOC/MDR is acceptable, provided the arrangement meets Section 5.6 (disclosure, NCA's prior written consent, and flow-down of Section 5 obligations) and personnel meet Section 5.10. A disclosed function with no access to NCA systems or data is outside the restriction but must be identified in the response. This requirement reflects NCA's federal data-residency and safeguarding obligations and applies uniformly to all non-U.S. delivery. For clarity, alert content, security telemetry, and ticket content are NCA data. Monitoring, alert intake, or ticket triage that involves viewing such content falls inside the Section 5.10 requirement regardless of whether the personnel hold system credentials. Only functions with no access to NCA systems or data of any kind sit outside the restriction, and any such function must be identified in the response.

Q. What are the expected support hours, and does 24/7 apply to the service desk or only to security?

Staff work across U.S. time zones (Eastern through Pacific); respondents should propose a coverage window suited to a distributed workforce. The 24/7 requirement covers threat monitoring and incident response. Security engineering and executive escalation are expected within the overall engagement but are not 24/7 functions. After-hours coverage applies to critical incidents; routine requests are handled in standard coverage hours, and after-hours demand has historically been low.

Q. What functions does internal IT retain, and what continuity coverage is expected during an absence of the Technology Manager?

Internal IT retains identity ownership, access-governance decisions, approvals, prioritization, and certain routine administrative actions (Section 3), and directs the partner's day-to-day work; the detailed responsibility matrix is finalized during onboarding. For continuity, NCA seeks a named backup resource from the partner who can assume the internal lead's essential day-to-day functions during an absence (planned leave or transition gap) so NCA is never single-threaded on any critical function. This is continuity coverage, not full operational takeover; business ownership remains with NCA. Describe and price your model.

Q. What business review cadence and reporting does NCA expect?

NCA expects a quarterly business review covering service performance against Section 9, security posture reporting including Microsoft Secure Score trends with regressions shown, and roadmap items. Reporting format may be proposed.

Environment, Assets & Licensing

Q. Please confirm users in scope and provide an asset inventory.

Approximately 50 full-time staff, all in scope, plus a small number of shared and service accounts to be inventoried during Phase 1. The endpoint fleet is approximately 50 organization-owned Windows laptops, mid-refresh on current-generation Dell hardware under manufacturer warranty (Section 4.9). Mobile devices are personal (BYOD) with limited access to NCA resources. Permitted BYOD access scenarios and any exception devices are confirmed during Phase 1 discovery. Azure-hosted resources are out of scope (Section 2). A complete asset and configuration inventory is a Phase 1 deliverable.

Q. Are all endpoints enrolled in Intune/Defender, and what is the licensing model?

All active devices are enrolled in and managed through Intune, with MFA enforced organization-wide and Conditional Access in place. Core licensing is Microsoft 365 Business Premium (nonprofit program) with select add-ons; endpoint and email protection run on the capabilities included in current licensing. Defender for Endpoint Plan 2 and Defender for Office 365 Plan 2 are not broadly deployed today. Respondents should propose against current licensing and may present licensing changes as separately priced options (Section 4.14). Coverage percentages and current-state detail will be shared with the selected partner during discovery.

Q. What key business applications require ongoing administration or support?

The primary platforms are listed in Section 2: the Microsoft 365 environment and named SaaS applications — hands-on admin-level assistance for Adobe Acrobat/Creative Cloud and Zoom, and escalation coordination plus admin-console configuration for vendor-supported platforms (Teamflect, DataSnipper, Mailchimp, Higher Logic). The full application inventory is confirmed during Phase 1. The Azure-hosted environment is out of scope.

Security Tooling & Operations

Q. What tools are in place beyond the Microsoft stack, and may respondents propose additional or dedicated tooling?

NCA operates a Microsoft-native stack and intends to standardize on it (Section 4.14). Any existing third-party tooling will be reviewed with the selected partner during discovery; no third-party product is mandated for retention beyond the Microsoft stack. Respondents proposing additional tools (including a dedicated vulnerability/patch or other platform) must identify, justify against the Microsoft-native alternative, and separately price them in the Section 10 layers. NCA reserves the right to accept or decline any additional tool.

Q. Is the requirement monitoring-only or full incident response, and what authority will the provider have?

Full lifecycle is expected: monitoring, investigation, containment, eradication, recovery, and remediation support (Section 4.7). NCA expects the provider to take direct containment actions under a pre-authorized playbook defined jointly during onboarding, with escalation boundaries and NCA notification consistent with the 24-hour standard in Section 5.3. Current incident-response documentation will be reviewed and matured with the selected partner as part of the Phase 1 baseline. Tabletop exercises and IR testing may be proposed, priced per Section 10.

Q. Are historical security metrics available, and what SOC/MDR model is acceptable?

NCA is not sharing security-operations metrics at this stage; respondents should size the program against the environment profile in Section 2 (approximately 50 users and 50 endpoints in a cloud-only Microsoft 365 environment). A shared SOC/MDR service model is acceptable, provided the named account-team requirement (Attachment B, Q9.1) is met and the Section 9 response commitments are satisfied.

Q. What is the current maturity of NCA's Purview and DLP configuration, and should respondents anticipate tuning existing policies or net-new implementation?

Current Purview and DLP configuration is current-state detail shared with the selected partner during Phase 1. Respondents should describe their capability across both scenarios, assessing and tuning existing policies and designing net-new ones, and should scope against current Business Premium licensing per the Section 2 clarification.

Vulnerability, Backup & Continuity

Q. Are vulnerability scans required, are remediation SLAs defined, and is penetration testing expected?

Respondents should propose their scanning approach, cadence, and remediation SLAs by severity (Section 4.4); NCA has not predefined remediation SLAs and will finalize them with the selected partner. Penetration testing is not required in the base scope and may be offered as separately priced optional work.

Q. Is there a third-party M365 backup, what retention is required, and are RTO/RPO defined?

Current-state backup tooling will be shared with the selected partner during discovery; respondents should price the Section 4.8 backup service in line with Section 4.14 tooling principles. Respondents

should propose retention periods per workload (consistent with Section 5.4 retention and legal-hold requirements) and state the RTO/RPO their solution supports; targets are finalized in the Phase 1 baseline.

Identity, Access & Compliance

Q. Is PIM implemented, how many privileged accounts exist, and what access-review cadence is expected?

Current privileged-access configuration detail will be shared with the selected partner during onboarding. Respondents should describe their own privileged-access model (Section 4.6) — standing versus just-in-time elevation, session logging, and a recommended access-review cadence for an organization of this size. Governing privileged access is an expected early workstream, and NCA expects periodic reviews (at least quarterly for privileged access) going forward.

Q. Which frameworks does NCA follow, and are policies/evidence in place or to be established?

NCA aligns to the frameworks named in Section 5.8 (NIST Cybersecurity Framework and NIST SP 800-171, with HIPAA where PHI is handled); NCA is not formally certified. The selected provider is expected to help establish, document, and mature controls and evidence; continuous evidence collection and control monitoring are in scope under Layer 2 (Section 10). Security awareness training is handled internally today, and the selected provider is expected to propose and operate the ongoing program, including phishing simulations, coordinated with internal IT.

Q. Has NCA had a prior IT, security, or governance assessment, and can findings be shared with respondents?

NCA is not distributing assessment history or findings to respondents. Any relevant materials are part of the current-state information provided to the selected partner under NDA during Phase 1.

Q. What is the annual compliance workload, and are there current gaps the provider will remediate?

On a typical annual basis NCA undergoes one external financial-statement/single audit that includes IT general controls (for example, verifying devices are compliant in Intune) and one insurance-related security review. Under Layer 2, NCA expects the partner to lead evidence collection, control monitoring, and audit documentation, while internal IT owns decisions, policy approval, and organizational context. NCA will not characterize current findings or gaps in this forum; the Phase 1 baseline (Section 4.1) establishes current state and drives the remediation roadmap.

Hardware, Service Desk Metrics & Transition

Q. What is the monthly ticket volume and tier distribution?

NCA averages approximately 25 in-scope tickets per month based on internal tracking. Approximately 60–65% resolve at Tier 1, 25–30% at Tier 2, and 5–10% at Tier 3. Typical requests span identity/access changes, Microsoft 365 and SharePoint support, endpoint and peripheral issues, standard software support (Adobe, Zoom), Teams and Teams Phone, and equipment logistics.

Q. What ticketing platform is in use today?

NCA maintains a lightweight internal intake and tracking process rather than an enterprise PSA. Respondents should propose their own platform and describe how it coordinates with internal intake, including the ticket-data feed into NCA's environment described in Section 4.3.

Q. What is the annual hardware lifecycle activity, and does nationwide recovery apply?

Approximately 10–15 combined onboarding and offboarding events occur annually, varying by year; replacements and returns beyond that follow the refresh cycle and warranty events. All staff are remote across the United States, so the Section 4.9 return logistics (prepaid shipping, tracking, and wipe verification) apply nationwide. Zero-touch provisioning via Autopilot/Intune is the deployment standard; current fleet enrollment state will be confirmed during discovery.

Q. Should hardware procurement and logistics be included in pricing?

Hardware is procured directly by NCA on its own vendor accounts. The partner's role is procurement coordination and the Section 4.9 lifecycle logistics, staging, deployment, recovery, and wipe verification, included in core Layer 1 pricing. Any pass-through costs are shown separately per Section 10.

Q. Is Salesforce administration in scope?

No. NCA is mid-implementation on a Salesforce-based AMS; vendor scope is limited to Microsoft 365 integration touchpoints (SSO via Entra, license provisioning/deprovisioning automation, conditional access). Day-to-day Salesforce administration sits with the AMS implementation team and internal IT.

Q. Is there an incumbent provider, and are there transition requirements?

No incumbent. These functions are currently handled internally, so onboarding is a transition from internal IT rather than a provider handoff, beginning with the Section 4.1 discovery and baseline. The Section 8 transition expectations apply at the end of the engagement.

Proposal & Pricing Requirements

Q. Is SOC 2 Type II mandatory or preferred?

Preferred. Respondents without a SOC 2 Type II may submit an equivalent assurance package per Section 5.7 (security questionnaire, willingness to sit for a control assessment, subprocessor attestations under NDA, and framework alignment). NCA retains discretion to determine sufficiency.

Q. Is pricing per-user or per-device, and how should MDR and project work be priced?

Core co-managed services are priced on a fixed per-user, per-month basis (Section 10); device-based or floor invoicing is not the required basis. MDR/SOC is priced separately as Layer 2 (per user or a flat monthly amount — state which and what it includes). Provide an hourly rate for out-of-scope project work; fixed-price statements of work may be agreed for defined projects by mutual consent.

Q. Is a performance or security bond required, and must references be from nonprofit clients?

No performance or security bond is required. At least three references must be from nonprofit clients of comparable size and environment, with at least one a current co-managed engagement (Attachment B, 8.2). Additional commercial references may be included, but the nonprofit references are required.

Q. Can NCA share context on the increased cybersecurity focus?

NCA is a federally funded organization handling sensitive constituent, employee, financial, and grant data, with growing safeguarding expectations for federal grantees. This solicitation reflects NCA's priority on a security-forward, continuity-minded co-managed partnership that strengthens NCA's posture while working alongside internal IT.