National Children's Alliance

Co-Managed Information Technology Services

Request for Proposal

(RFP No. NCA-IT-2026-02)

RFP COORDINATOR
Jennifer Read, Controller
National Children's Alliance
921 Pennsylvania Avenue SE, Washington, DC 20003
jread@nca-online.org

TECHNICAL LIAISON
Precious Eze, Technology Manager

ISSUE DATE
September 1, 2026

TABLE OF CONTENTS

1. Introduction

National Children's Alliance (NCA) is pleased to invite qualified, nonprofit-experienced providers to respond to this Request for Proposal (RFP) for co-managed information technology services. The intent of this RFP is to solicit proposals from qualified providers and to select a partner to work alongside NCA's internal technology staff.

1.1 About National Children's Alliance

NCA is the national accrediting body and membership organization for Children's Advocacy Centers (CACs) across the United States, supporting a network of more than 300 member CACs and state chapters. As a pass-through grantmaking entity and membership organization whose revenue is predominantly federal (primarily U.S. Department of Justice / OJJDP awards), NCA operates with a high standard of accountability for both donor and federal taxpayer resources. NCA runs a lean, fully remote workforce on a November 1–October 31 fiscal year.

1.2 Purpose & Scope

NCA seeks a **co-managed IT services partner** to work **alongside our internal technology staff** — not to replace them, and not to operate as a hands-off, black-box helpdesk. The partner provides day-to-day end-user support along with the advanced engineering and security layer, supplementing and extending our internal capacity, while NCA's internal IT remains the day-to-day organization-side owner — retaining context, approvals, prioritization, and certain routine administrative actions, and directing the partner's work. NCA retains ownership of its identity environment, governance, and technology direction, and the partner is expected to integrate through shared tooling and documentation, escalate and transfer knowledge cleanly, and stay actively coordinated with internal staff.

Predictable, transparent, nonprofit-conscious pricing is a core requirement. This RFP is issued for evaluation and planning purposes and does not commit NCA to contract for any service. NCA will not reimburse any costs incurred in responding; all such costs reside with the responding party.

1.3 Confidentiality Statement

All information included in this RFP is considered confidential and intended only for use by responders. No information included in this document, or in discussions related to NCA's provider selection effort, may be disclosed to another party or used for any other purpose without NCA's express written consent.

2. Environment Overview

NCA operates a modern, cloud-native environment with **no on-premises servers, no data center, and no on-site network infrastructure to maintain.**

This is an established, actively managed environment, not a greenfield build. Microsoft 365 (E5-level) is fully deployed and in active use — Entra ID, Intune, Defender, and Purview — with multi-factor authentication enforced organization-wide, Conditional Access in place, and all active devices enrolled in and managed through Intune. Respondents should propose to extend, harden, and mature this

environment, and should anticipate an initial assessment and standardization phase rather than a from-scratch implementation.

Workforce: Approximately 50 full-time employees, 100% remote, working across multiple U.S. time zones. There is no central office for IT support; all support is delivered remotely.

Cloud platforms:

- **Microsoft 365** (advanced security/compliance entitlements — Entra ID, Intune, Defender, and Purview suites; Teams with Teams Phone; select Copilot / Power BI Premium licensing)
- **Microsoft Entra ID** — cloud identity provider (SSO, conditional access, MFA)
- **SharePoint Online / OneDrive** — cloud file storage and collaboration
- **Microsoft Teams** — collaboration and cloud telephony (Teams Phone, within M365 licensing)
- **Microsoft Intune** — endpoint / mobile device management
- **Microsoft Defender** — endpoint and email threat protection
- **Microsoft Purview** — data governance, retention, eDiscovery, and legal hold

Endpoint fleet: ~50 organization-owned Windows laptops plus peripherals, all in remote home offices. Asset procurement, provisioning, tracking, and return logistics for remote and departing staff are an active priority.

Internal IT footprint: One internal IT staff member (Technology Manager) serving as the organization-side liaison; strategic and budget decisions are made by NCA leadership.

Azure footprint: NCA also maintains limited Azure-hosted resources (a REDCap/MySQL research database and associated VPN/VNet). These are managed under a separate arrangement and are out of scope for this engagement, but are noted so vendors account for them during discovery.

Additional SaaS applications: Beyond Microsoft 365, the partner will support other SaaS applications in daily use. Hands-on, admin-level assistance (e.g., reinstall/repair, license adjustments, common error patterns) is expected for Adobe Acrobat / Creative Cloud and Zoom. For vendor-supported platforms such as Teamflect, DataSnipper, Mailchimp, and Higher Logic, the partner coordinates escalations and performs admin-console configuration; strategic vendor relationships and policy-level escalations remain with internal IT.

Association Management System (AMS): NCA is mid-implementation on a Salesforce-based AMS. Vendor scope for Salesforce is limited to Microsoft 365 integration touchpoints (SSO via Entra, license provisioning/deprovisioning automation, and conditional access); day-to-day Salesforce administration and configuration sit with the AMS implementation team and internal IT.

3. Co-Managed Model & Division of Responsibilities

This engagement is structured as a co-managed partnership. The lists below set baseline expectations; final boundaries will be confirmed with the selected partner during onboarding. Internal IT remains the organization-side owner of IT context, approvals, and prioritization; the partner supplements and extends internal capacity

Internal IT retains (NCA-side):

- Day-to-day organization-side ownership — context, approvals, prioritization, and certain routine administrative actions — directing and coordinating the partner's day-to-day work
- Authorizing user account creation and de-provisioning (approvals and identity ownership)

- Access-governance decisions and ownership of the identity environment
- Internal point of contact for NCA-specific approvals and priorities

Asset receipt for returned, redeployed, and exception devices, and front-line coordination with staff (new devices are configured and drop-shipped by the partner directly to remote staff).

Vendor is expected to provide (Partner-side):

- Day-to-day end-user help/service desk (Tier 1 through Tier 3) that **supplements and extends internal capacity**, under internal IT's direction and prioritization: ticket intake, troubleshooting, break/fix, software and how-to support, and password/account assistance
- 24/7 cybersecurity monitoring and response (MDR / EDR)
- Mobile Device Management (MDM) orchestration and policy administration (Intune)
- Cloud infrastructure and Microsoft 365 data backup
- Patch and vulnerability management at scale
- Hardware procurement, zero-touch provisioning, and lifecycle/return logistics
- Documentation, runbooks, and knowledge transfer to internal staff

Shared / collaborative (jointly owned):

- Onboarding/offboarding workflows and automation design
- Microsoft 365 / Entra administration and license governance
- Security policy definition and incident response
- Technology planning and budgeting for the fiscal year

A central evaluation factor is **how cleanly the partner integrates with a single internal resource** — shared visibility, no "black box" administration, and a documented escalation handshake.

4. Scope of Work

4.1 Onboarding Discovery, Baseline & Standards Alignment (Phase 1). As the first phase, the partner will conduct a structured discovery and current-state review and produce a documented configuration baseline across identity (Entra ID), endpoint management (Intune), threat protection (Defender), data governance (Purview), backup, and access controls. Deliverables include a complete asset and configuration inventory; a documented security baseline mapped to recognized frameworks and federal grantee expectations (Section 5); and a prioritized roadmap to bring the environment to the partner's managed-service standard, with standardization and routine hardening implemented as part of onboarding. This baseline will also establish and document the IT general controls (access, change management, backup) that support NCA's ongoing financial-statement and single-audit readiness, and should inventory and deploy any new-but-undeployed equipment already on hand. Describe your discovery methodology, the frameworks you map to, the deliverables NCA receives, and your typical onboarding timeline.

4.2 Remote Monitoring & Management (RMM). Continuous monitoring of all endpoints and cloud services; automated alerting; health/performance dashboards visible to internal IT; proactive remediation. Describe your RMM platform and the NCA-side visibility you provide. Before proposing additional tooling, describe how you will use and integrate with NCA's existing Microsoft security and management stack (Defender, Intune, Entra, Purview); any additional RMM, MDR, backup, or security agents must be clearly justified and priced separately.

4.3 Co-Managed Service Desk & End-User Support (Tier 1–3). The partner delivers day-to-day end-user support that **supplements and extends internal capacity** — ticket intake across channels, troubleshooting, break/fix, software and how-to support, password/account assistance, and Tier 2/3 escalation engineering — operating under internal IT's direction and prioritization, with internal IT remaining the organization-side owner for context, approvals, and certain routine administrative actions. Define your ticketing/PSA platform and how it coordinates with our internal intake so we maintain one coherent view of tickets; your escalation intake and hand-back; first-contact resolution; and how end users are kept informed. Describe coverage hours, after-hours/on-call handling, target response/resolution times by priority, and support for a multi-time-zone workforce. The partner must also provide NCA-side visibility into ticket data in real time — ideally via a feed or export into NCA's environment (dashboard, API, or scheduled export) rather than requiring a separate login to the partner's platform — so internal IT can independently track volume, trends, and status.

4.4 Patch & Vulnerability Management. Patch orchestration for OS and third-party applications across a fully remote fleet (via Intune/cloud); patch ring/test strategy; vulnerability scanning and remediation SLAs; reporting cadence.

4.5 Endpoint & Mobile Device Management (MDM). Assess the current Intune configuration, bring it to a documented managed standard, and administer it on an ongoing basis: compliance policies, configuration profiles, app deployment, encryption (BitLocker) enforcement, conditional-access integration, and remote wipe. Address organization-owned laptops and, where applicable, mobile access to NCA resources.

4.6 Identity & Access Management. Entra ID administration: conditional access, MFA, SSO, privileged access management, and access reviews. Describe how you co-administer identity without sole/opaque control of our tenant, including your privileged access model for partner staff, standing admin accounts versus just-in-time elevation, approval workflow, session logging or recording, and how partner access is reviewed and revoked.

4.7 Cybersecurity (MDR / EDR / Response). 24/7 managed detection and response; endpoint detection and response (Defender or equivalent); email security/anti-phishing; SIEM/log management; security awareness training and phishing simulation; and a defined incident response process with breach-notification commitments (Section 5). Specify SOC staffing and response-time commitments.

4.8 Backup & Business Continuity. Third-party backup of Microsoft 365 data (Exchange, SharePoint, OneDrive, Teams) independent of Microsoft-native retention; backup frequency, retention, and tested restore process; documented RPO/RTO for cloud data and identity; and a business continuity / disaster recovery approach for a cloud-only organization.

4.9 Hardware Procurement, Provisioning & Lifecycle (Remote Staff). NCA is currently completing a fleet refresh with Dell Pro / Pro Max laptops, with units already in service or in stock under manufacturer ProSupport / ProSupport Plus coverage held by NCA. The partner steps into a refresh-in-progress rather than a greenfield buildout. Scope includes zero-touch deployment (Windows Autopilot / Intune) of new machines drop-shipped to remote employees; standardized imaging/configuration; asset tagging and inventory; **coordination of the manufacturer warranties NCA already holds — opening and managing Dell ProSupport cases and RMAs — without duplicating hardware break/fix coverage in the partner's fee;** and return logistics for departing/relocating staff (prepaid return shipping, tracking, data-wipe verification with certificate of destruction for data-bearing devices, and redeployment of good-condition units). For remaining or future purchases, NCA may buy hardware directly on nonprofit pricing; respondents should price **both** a provisioning-only model (NCA procures, partner configures/enrolls) **and** full procurement with markup (Section 10). Timely, verifiable equipment return is a known priority — describe your process specifically.

4.10 Microsoft 365 Administration & License Optimization. Tenant administration and health; nonprofit licensing optimization (Microsoft nonprofit grants/discounts, right-sizing entitlements, eliminating license sprawl). NCA expects a partner who actively reduces unnecessary licensing cost rather than maintaining the status quo.

4.11 Onboarding / Offboarding Automation. Co-design repeatable, auditable provisioning/de-provisioning workflows — license assignment/removal, group/permission changes, mailbox conversion, data preservation, and timely access revocation. Describe automation you can bring.

4.12 Documentation & Knowledge Management. Maintained, NCA-accessible documentation (environment, configurations, runbooks, asset inventory). NCA retains full ownership of and unrestricted access to all documentation, credentials, and configurations at all times and at the end of the engagement (Section 8).

4.13 Reporting. Regular reporting on tickets/SLAs, security posture, patch compliance, backup status, and asset inventory, plus periodic executive summaries suitable for leadership and board reference.

4.14 Tooling Principles (leverage existing stack; no lock-in). NCA operates a Microsoft-native environment and prefers solutions that use the licensing and capabilities NCA already owns (Entra ID, Intune, Defender, Purview) before introducing third-party tools. The following principles apply:

- Any additional or proprietary tooling (e.g., RMM, MDR/SOC, SIEM, patching, backup, documentation, or ticketing) must be individually identified and justified against the Microsoft-native alternative, and separately priced in the Section 10 pricing layers so NCA can evaluate incremental cost and value.
- For each proposed tool, state whether it is included in the recurring fee or billed separately, whether the license is NCA-owned or partner-provided, and what becomes of that capability, its configuration, and its data at contract termination.
- NCA reserves the right to accept or decline any proposed additional tool and to require use of its existing Microsoft capabilities where NCA determines they are sufficient. Proposing to bundle proprietary tooling does not obligate NCA to adopt or pay for it.
- NCA will hold its own administrative access to every platform, agent, or console deployed in or against its environment, including RMM, MDR, backup, and ticketing. The partner may not deploy

any tool that stores NCA data or configurations in a system NCA cannot independently access, and must disclose every tool before deployment.

- Describe your ability to provide surge or backfill coverage when NCA's internal IT lead is unavailable (e.g., leave or transition), so that NCA is never single-threaded on any critical function. Continuity of operations is a priority for NCA given a lean internal team.

5. Security, Data Protection & Compliance

NCA handles sensitive information, including employee and constituent **personally identifiable information (PII)**, financial and payroll/HR data, member and accreditation records, **federal grant data subject to federal safeguarding expectations**, and potentially **protected health information (PHI)**. Respondents must address each item below.

5.1 Endpoint security (remote workforce). Full-disk encryption, MFA/conditional-access enforcement, endpoint hardening, and protection of devices operating entirely outside any corporate network perimeter.

5.2 Required safeguards. Administrative, technical, and physical safeguards consistent with industry standards and applicable law, including at minimum: (a) access controls and least privilege; (b) strong authentication; (c) encryption in transit and at rest for PII and PHI where feasible; (d) secure configuration, patching, and malware protection; (e) logging and monitoring; (f) secure software/administration practices; and (g) personnel security and training. Describe how you meet each.

5.3 Security incident notification. Notify NCA in writing **without undue delay and no later than 24 hours after discovery** of any actual or reasonably suspected unauthorized access, acquisition, use, disclosure, alteration, or destruction of NCA data, PII, or PHI — including known details, mitigation, and corrective actions — and cooperate with NCA's investigation, notifications, and remediation. Confirm your ability to meet this 24-hour standard.

5.4 Data governance, retention & eDiscovery. Support for data loss prevention, retention, and eDiscovery / legal hold (Purview). NCA periodically requires litigation hold and audit/eDiscovery capability and expects partner fluency.

5.5 No secondary use; data minimization. The partner shall not access, use, disclose, or process NCA data for any purpose other than performing the services, shall access only the minimum data necessary, and shall not perform data mining or any secondary use of NCA data.

5.6 Subcontractors / fourth parties. No subcontracting of services involving access to NCA systems, PII, or PHI without NCA's prior written consent and a written agreement binding the subcontractor to protections at least as stringent. Disclose anticipated subcontractors.

5.7 Vendor security posture. A current SOC 2 Type II report is preferred. Where a respondent does not hold a SOC 2 Type II, NCA will consider an equivalent assurance package, which may include: (a) completion of NCA's security questionnaire; (b) willingness to participate in a control assessment on reasonable notice; (c) current SOC 2 / ISO or comparable attestations from the respondent's material security subprocessors (e.g., MDR, backup, RMM), available under NDA; and (d) demonstrated alignment to a recognized framework (NIST SP 800-171 Rev 3 or CIS). Respondents should also describe internal controls, personnel background screening, and access governance for staff who will touch NCA

systems. NCA retains sole discretion to determine whether an assurance package adequately addresses its requirements.

5.8 Framework alignment (federal grantee standard). NCA expects security practices consistent with those expected of federal grantees, including alignment with the **NIST Cybersecurity Framework and/or NIST SP 800-171**; safeguarding of protected PII consistent with **2 CFR 200.303**; the IT security expectations of the **DOJ Financial Guide**; and internal control practices consistent with the **GAO Green Book / COSO** framework. Describe how you would help NCA establish, document, and maintain controls to this standard.

5.9 HIPAA / Business Associate Agreement. To the extent the partner creates, receives, maintains, or transmits PHI on NCA's behalf, the partner must execute a **Business Associate Agreement (BAA)** and comply with the HIPAA Security Rule (45 C.F.R. Part 164, Subpart C), including breach reporting under 45 C.F.R. § 164.410. Confirm ability and willingness to execute a BAA.

5.10 Data residency & U.S.-based support. Confirm U.S. data residency for NCA data. All service desk, security operations (SOC/MDR), and administrative support functions that access NCA systems or data must be performed by U.S.-based personnel; identify any function performed outside the United States or by a subcontractor, and the safeguards that apply. Confirm willingness to sign NCA's confidentiality agreement (Section 8).

6. Federal Procurement & Contracting Requirements

Because NCA's funding is predominantly federal and these services will be treated as a federally funded **indirect cost**, the selected vendor must meet federal procurement and flow-down requirements. This competitive solicitation and the resulting documentation are intended to support the allowability and reasonableness of the cost under 2 CFR Part 200. Respondents must:

- Maintain an active **SAM.gov registration** with a **Unique Entity ID (UEI)** prior to contract award. A respondent whose registration is pending at proposal submission may respond by indicating its registration status; active registration is a condition of award, not of submission.
- Certify they are **not suspended, debarred, or otherwise excluded** from federal programs (2 CFR Part 180 / 200.214).
- Provide **itemized, transparent invoicing** sufficient to support cost reasonableness and treatment as an allowable indirect cost.
- Maintain accurate service and billing records for **at least three (3) years** and make them available, on reasonable notice, for NCA (and, where applicable, federal) inspection and audit.
- Accept applicable **federal contract provisions** (2 CFR Part 200, Appendix II) as applicable to a federally funded engagement, and standard nonprofit terms.
- Disclose any conflicts of interest, and any current or prior employment, contractor, or business relationship with NCA (including prior access to NCA systems or credentials). NCA reserves the right to evaluate respondent independence — particularly with respect to the assessment in Section 4.1 — and to require appropriate safeguards.

NCA reserves the right to request a cost or price breakdown to document a fair and reasonable price.

7. Insurance Requirements

The selected partner shall maintain, at its own expense for the term, insurance appropriate to the services and provide certificates of insurance upon request. Confirm you carry, or can obtain, the following:

- **Commercial General Liability** — $1,000,000 per occurrence / $2,000,000 aggregate
- **Technology Errors & Omissions / Professional Liability** — $2,000,000 per claim / $2,000,000 aggregate
- **Cyber & Privacy Liability**, including breaches of PII and PHI and regulatory proceedings — $2,000,000 per claim / $2,000,000 aggregate
- **Workers' Compensation and Employers' Liability** — as required by applicable law (Employers' Liability of at least $500,000)

NCA may request to be named as an additional insured where appropriate. State any coverage you do not currently carry.

8. Anticipated Contract Terms (Master Services Agreement)

The engagement will be governed by a master services agreement (MSA) with statements of work. Key terms NCA will expect are summarized below; respondents should note any term they cannot accept and should submit a copy of their proposed MSA with their response.

- **Ownership of work product.** Deliverables, configurations, documentation, scripts, and reports created for NCA are owned by NCA (work made for hire or by assignment upon payment). The partner may retain pre-existing tools/know-how but grants NCA a perpetual, royalty-free license to use them as embedded in NCA's deliverables and environment. NCA retains full ownership of and access to all credentials, tenant configurations, and documentation at all times and upon termination.
- **Confidentiality.** Mutual confidentiality covering NCA's financial, operational, security, personnel, member, vendor, and system information, surviving termination.
- **Data protection & BAA.** The safeguards, 24-hour incident notification, and BAA obligations in Section 5.
- **Standard of care & warranty.** Services performed in a professional, workmanlike manner consistent with industry standards and applicable law, with correction of material nonconformities at no additional charge for a defined warranty period.
- **Termination.** For convenience on 90 days' written notice by either party; for cause with a 15-day cure period; and NCA's right to suspend access immediately for security, privacy, legal, or risk reasons.
- **Records & audit.** Service and billing records retained three years and available for inspection (Section 6).
- **Indemnification & limitation of liability.** Partner indemnification for breaches, negligence/willful misconduct, violations of law, IP infringement by deliverables, and security incidents caused by the partner's failure to meet its security obligations; mutual limitation of liability with carve-outs for confidentiality, data protection, indemnification, infringement, and willful misconduct.
- **Governing law & venue.** District of Columbia law; exclusive venue in the District of Columbia; prevailing-party attorneys' fees.

- **Transition assistance.** Reasonable cooperation to transition systems, knowledge, credentials, and data to NCA or a successor provider at the end of the engagement. Where the partner provided proprietary tooling (e.g., MDR, patching, backup), the partner will identify NCA data and configurations held in that tooling and provide them to NCA (or its successor) in a usable format, and cooperate to avoid any lapse in security monitoring, patching, or backup during transition.

9. Service Level Expectations (SLAs)

Respondents should propose SLAs and confirm ability to meet or exceed the following; final SLAs will be incorporated into the contract.

- **Critical (business-down / security incident):** acknowledge within 15–30 min; active response 24/7.
- **High:** acknowledge within 1 hour during coverage hours.
- **Standard:** acknowledge within 4 business hours.
- **Coverage hours:** define standard support window and after-hours/on-call.
- **Reporting:** monthly SLA performance reporting; quarterly business review.

10. Pricing Model

NCA requires **predictable, fixed recurring pricing.** Core co-managed services should be priced on a fixed per-user, per-month basis; avoid variable/hourly-only structures for core managed services. Respondents must present pricing in clearly separated layers so that bids are comparable and each layer's cost is transparent:

- Layer 1 — Core co-managed services (per user, per month): service desk and escalation, Microsoft 365 and Entra administration, endpoint management, backup, hardware provisioning and return logistics, and standard support.
- Layer 2 — Security & continuity program: 24/7 monitoring / MDR and identity threat detection, incident response, vulnerability management, and the federal-grant compliance/evidence workload (framework maintenance, continuous evidence collection, policy lifecycle, and responses to security questionnaires and control assessments). This layer may be priced per user or as a separate flat monthly amount — state which, and what it includes.
- One-time onboarding / transition, stated separately.

Item	Basis	Cost
Layer 1 – Core co-managed services		
Core co-managed services - service desk, escalation, M365/Entra administration, endpoint management, Microsoft 365 backup, and hardware provisioning/return logistics	per user / month	$
Layer 2 – Security & continuity program		
Security operations — MDR/EDR, identity threat detection, incident response, and vulnerability management	per user or flat / month	$
Compliance & evidence program — framework maintenance, continuous evidence collection, policy lifecycle, and responses to security questionnaires/control	flat / month	$

assessments		
One-time & variable		
One-time onboarding / Phase 1 discovery & baseline	Flat	$
After-hours / on-call support	rate or included?	$
Project work (out of scope)	hourly rate	$
Hardware provisioning only (NCA procures)	per device	$
Hardware full procurement (partner buys)	markup % / flat fee	$
Pass-through tooling / licensing	at cost?	$

- **Explicitly call out any onboarding fees and any after-hours fees** (or confirm they are included).
- State your **nonprofit pricing** or sector discount.
- Propose your **contract term and any flexibility** (note the 90-day termination-for-convenience expectation in Section 8).
- Confirm pricing is held for the initial term and describe any annual escalator.
- Clearly distinguish services included in the fixed monthly fee from those treated as billable project work or out-of-scope, with common examples.

11. Response Process

11.1 Clarifying Questions

Submit written clarifying questions to the RFP Coordinator by the date in Section 13. Answers will be compiled and shared with all known respondents.

11.2 Primary RFP Contact

Jennifer Read, Controller — jread@nca-online.org — National Children's Alliance, 921 Pennsylvania Avenue SE, Washington, DC 20003. Technical liaison: Precious Eze, Technology Manager. All inquiries in writing.

11.3 Response Delivery Instructions

Submit responses by email to jread@nca-online.org with the subject line "NCA-IT-2026-02 — Co-Managed IT Proposal — [Vendor Name]" no later than the deadline in Section 13. Include: completed **Attachment A** (Corporate Information) and **Attachment B** (Questions); a proposal narrative addressing Sections 4–10; a completed pricing table (Section 10); your proposed **Master Services Agreement**; SOC 2 Type II report (or equivalent, may be under NDA); a sample monthly/QBR report; at least three nonprofit references; a certificate of insurance; and SAM.gov UEI. Responses should be concise.

12. Selection Criteria & Process

12.1 Selection Criteria

NCA will select the best overall solution and is not obligated to select the lowest-priced respondent. Weighted criteria:

Criterion	Weight
Technical expertise (Microsoft 365 / security stack depth; onboarding & baseline approach)	20%
Security & compliance posture (SOC 2, frameworks, federal fit)	20%
Co-managed collaboration model (integration with internal IT)	20%
Pricing & value (predictability, transparency, total cost)	20%
Service delivery & remote support capability (SLAs, coverage, time zones)	10%
Relevant experience & past performance (nonprofit and federally funded clients; comparable size and cloud-only environment; references)	10%

12.2 Selection Process

Responses will be reviewed and scored against the criteria above, with clarification requested as needed. NCA will identify two to three finalists for in-depth review, including interviews/demonstrations and reference checks.

12.3 Finalist Presentations

Finalist presentations/demonstrations will be held virtually on the dates in Section 13; NCA will provide finalists as much advance notice as possible.

13. Key Dates

Task	Date
RFP issued	Tuesday, September 1, 2026
Written questions due	Wednesday, September 9, 2026 (5:00 PM ET)
NCA responses to questions posted	Monday, September 14, 2026
Proposals due	Tuesday, September 22, 2026 (5:00 PM ET)
Finalist interviews/demos	Week of October 5, 2026
Selection & contract execution	Mid-to-late October 2026
Onboarding begins	Early November 2026

14. General Terms

- This RFP is not an offer or a commitment to contract. NCA may decline to award, may award to other than the lowest-priced respondent, and may negotiate with one or more respondents.
- All costs of responding are borne by the respondent.
- NCA may request clarifications and additional information.
- This RFP and all submissions are confidential to the evaluation process.
- NCA reserves the right to amend or cancel this RFP at any time.

Attachment A — Response Form: Corporate Information

Please complete the table below. Use "NA" where not applicable.

1.1 Company Name	
1.2 Company Address	
1.3 Contact for this RFP (name, title, phone, email)	
1.4 Company Website	
1.5 Main Products / Services	
1.6 Main Market / Customers (note % nonprofit)	
1.7 Number of Years in Business	
1.8 Company Location(s)	
1.9 Total Employees (2023 / 2024 / 2025)	
1.10 Employees in Technical Support / SOC	
1.11 Clients of Comparable Size (40–60 users; cloud-only)	
1.12 Subsidiaries, Affiliations, Partnerships (incl. Microsoft partner status)	
1.13 SAM.gov Unique Entity ID (UEI) — if registered; otherwise indicate registration status	
1.14 Not Suspended/Debarred/Excluded (certify Y/N)	
1.15 SOC 2 Type II current? (Y/N + date)	
1.16 Willing to execute a BAA (Y/N)	
1.17 Confirm insurance coverages per Section 7 (Y/N)	

Attachment B — Response Form: Questions

Please answer each question directly in the answer row beneath it. Keep answers concise.

1.0 General

Q1.1 What types of organizations do your clients represent, and what percentage are nonprofits?

Q1.2 Why are you a good fit for fully remote nonprofit of ~50 staff?

Q1.3 Do you conduct quarterly or semi-annual business reviews, and what do they cover?

2.0 Independence

Q2.1 Disclose any current or prior employment, contractor, or business relationship between your firm (or its personnel) and NCA, including any prior access to NCA systems or credentials. How would you ensure an independent, objective assessment of NCA's environment (Section 4.1)?

3.0 Co-Managed Collaboration

Q3.1 Describe your co-managed delivery model. How do you divide responsibilities with a client's single internal IT resource without taking over or sidelining that person?

Q3.2 How do you ensure shared visibility (no "black box")? What does our internal staff member see and control day to day?

Q3.3 Describe your escalation workflow when our internal resource hands an issue to you — and how it is handed back.

4.0 Onboarding & Assessment

Q4.1 Describe your onboarding discovery and baseline assessment methodology (Section 4.1): frameworks you map to, deliverables NCA receives, how you implement standardization/hardening during onboarding, and your typical timeline.

5.0 Tooling & Integration

Q5.1 What PSA/ticketing platform do you use, and how does it integrate or coordinate with our internal intake so we have one coherent view of tickets? Can you feed or export ticket data into NCA's environment so internal IT can independently track volume, trends, and status in real time?

Q5.2 What RMM and security tooling do you deploy, and is any of it left behind / transferable if we part ways?

6.0 Remote-First & Microsoft Depth

Q6.1 Describe your experience supporting fully remote, multi-time-zone organizations with no central office.

Q6.2 Describe the depth of your Microsoft 365 / Entra / Intune / Defender / Purview expertise, with certifications and Microsoft partner status.

Q6.3 Describe your Autopilot / zero-touch provisioning process for drop-shipping configured laptops to remote employees, and your equipment return/recovery process for departing staff.

7.0 Security & Continuity

Q7.1 Describe your 24/7 SOC/MDR capability and staffing model.

Q7.2 Summarize a recent incident you managed end to end (anonymized) and the outcome.

Q7.3 Describe your M365 backup solution and a recent tested restore from a production client environment, including scope, data volume, duration, outcome, and sign-off.

Q7.4 Confirm your ability to meet the 24-hour incident notification standard (5.3) and to execute a BAA (5.9).

8.0 Nonprofit Fit & References

Q8.1 Describe your understanding of nonprofit budget realities and federal-grant compliance considerations.

Q8.2 Provide at least three references from nonprofit clients of similar size and environment at least one of which must be a current co-managed engagement

9.0 Staffing & Service

Q9.1 Who would be our named account team? What is their tenure and turnover?

Q9.2 What are your standard SLAs (Section 9) and how are they reported?

Please provide any other information you feel should be considered in our evaluation.