NEW MEXICO FINANCE AUTHORITY

QUESTIONS and ANSWERS TO REQUEST FOR PROPOSALS

INFORMATION TECHNOLOGY (IT) MANAGED SERVICE PROVIDER AND NETWORK OPERATIONS CENTER (NOC)

DATE ISSUED: October 23, 2025

Question: Please provide the locations to be managed and an overview diagram of the infrastructure.

Answer: Albuquerque Data Center (ABQDC) & Santa Fe Office Building (SF)

Question: Per location, please provide and/or describe an inventory of the networking elements to be supported (routers, switches, gateways, firewalls, end devices, servers) along with the model numbers, quantities, and maintenance levels.

Answer: Devices to Be Monitored

Device Type	Quantity	Manufacturer / Platform	Notes	Location
Physical Servers	2	Dell PowerEdge (Windows Server 2019/2022)	Legacy, DR support only	ABQ DC
Virtual Servers	10	Verge.io	Core apps & domain controllers	ABQ DC
Switches	8	Cisco Meraki MS series	Cloud-managed	ABQ DC - 2 Santa Fe - 6
Security Appliances	4	Cisco Meraki MX series	Primary + failover	ABQ DC - 2 Santa Fe - 2
Wireless Access Points	14	Cisco Meraki MR series	Cloud-managed	Santa Fe
Endpoints	160	Lenovo – laptops Dell – Desktops – Satan Fe	Windows 10/11 managed in Intune	Remote - laptops Santa Fe - Desktops
Mobile Devices	80	Apple	Managed via Intune MDM	Remote
Printers	4	Ricoh	Contacted out	Santa Fe
Conference room AV	4	Dell and various	TVs and Kiosks	Santa Fe

---

Question: The circuits to be monitored along with circuit types and speeds and associated carrier.

Answer: ISP Connections

Provider	link type	primaries	locations	Speeds
Comcast	Ethernet	Yes	"SF Office"	1000
Comcast	Ethernet	No	"Cyxtera Albuquerque Data Center"	1000
Comcast	Ethernet	No	"Cyxtera Albuquerque Data Center"	100
Comcast	Ethernet	Yes	"Shelby Building"	1000
Harmony SASE	SASE	No	"SF - San Mateo"	1000
Level 3	Ethernet	No	"Cyxtera Albuquerque Data	1000

			Center"	
Level 3	Ethernet	No	"Cyxtera Albuquerque Data Center"	100
Lumen	Ethernet	No	"Cyxtera Albuquerque Data Center"	100
Lumen	MPLS	No	"Cyxtera Albuquerque Data Center"	100
Lumen	MPLS	No	"Shelby Building"	100
Lumen	Other	No	"Shelby Building"	100
Lumen	Other	No	"Shelby Building"	100

ISP are managed by a combination of brokers and by NMFA. Deprecation is required for multiple lines to consolidate.

Question: The network architecture (e.g. SDWAN)

Answer: Meraki – SDWAN

Question: An inventory of any Wi-Fi equipment to be monitored.

Answer: Meraki Aps and SSIDs | Guest wireless

Question: An inventory of any mobile or IOT devices to be monitored

Answer: Printers and Conference rooms

Question: Any custom elements

Answer: Board Presentation software for Board room (Granicus) and Security System – Verkada

---

Question: Will you need us to provide carrier coordination for your circuits?

Answer: Yes, and you can replace it with renewal if cost is included.

Question: Will you need us to provide vendor (e.g. Cisco) coordination for networking devices?

Answer: Yes, we have Meraki infrastructure and support.

Question: Are there any current initiatives, in-flight projects or new solutions underway that need to be supported or that will have impact on our scope?

Answer: CIS Framework Coordination. Completion of ZTNA and other Security requirements. Hardware replacement and Data Management.

Question: Does NMFA have title to all equipment? Would NMFA be interested in options to rent the equipment from us?

Answer: Yes, and yes, based on life cycle schedule for replacement. Currently under lease and purchased but would like to lease all devices.

Question: Is maintenance current on all devices?

Answer: Yes

Question: Do you need us to manage the product life cycle for your equipment?

Answer: Yes, please manage and advise.

Question: Per access to your network for monitoring and managing purposes, what options will we have?

Answer: We utilize NinjaOne RMM and are open to utilizing tools that meet security requirements. Access can be provided with RBAC for whatever resource you require access to.

Question: We have a fully integrated platform with a complete set of tools to handle your scope. Are there any tools that you have that we need to integrate to?

Answer: Zendesk for ticketing, monitoring and collaboration. NinjaOne for RMM, Adlumin for SOC/SIEM, AutoElevate for JIT access, Harmony for ZTNA/SaSE, M365 for Intune and Entra, Verizon for cell phones, Apple Business Manager for cell phones, WebEx, Zoom, Teams for video and voice, and Auvik for anomalies detection, Auvik SaaS Management for SaaS monitoring, and AssetSonar fore asset management. Otherwise, we can specify the tools upon request of the specific type.

Question: Is US-based support a requirement?

Answer: TIER 1 – preferred, TEIR 2 – required TIER 3 – required

---

Question: Are there any network-based applications (e.g. VoIP, contact center) that we will need to support?

Answer: Zoom Meetings and WebEx phone systems.

Question: Please provide more information and details on the security related requirements.

Answer: CIS Framework compliant as goal

Question: Per license management and consolidation, please provide an inventory of current licenses. Types, versions, and quantities.

Answer: Assume 80+ licenses. M365 E5 – GCC (Visio, Exchange, Azure). CheckPoint Harmony. Cisco DUO. Adobe Pro. Adlumin SOC. Various IT system at less than 15 users.

Question: Is there any cloud connectivity that falls within the scope of these services? If yes, please describe.

Answer: Yes, our goal is cloud-first – all SaaS.

Question: Who is currently handling this scope of work now?

Answer: IT and Operational Excellence Teams.

Question: Does the work need to be done in NM, or is it open to another location?

Answer: No, the remote TIER 1 can be handled from any location, SLA and time frames of viability are requirements.

Question: What is the current size of the team?

Answer: Approaching 80 staff, 5 to 6 IT staff

Question: Do we know the volumes involved? Ie calls, tickets, weekly and monthly

Answer: In the past 30 days (10/06/2025 – 11/06/2025):
Incident tickets = 10, Tasks = 50, Problems = 0, Reporting or Questions = 500

Question: Are the expected SLAs defined?

Answer: Utilizing ITIL as the foundation, see Appendix A to these Questions and Answers

---

Question: What is the total number of supported users, physical locations, and remote staff included in the service scope?

Answer: Total users: ≈ 80 employees (including full-time, contractors, and program-specific staff). Physical locations: 1 primary office in Santa Fe, NM + 1 disaster-recovery co-location in Albuquerque (cloud-based via Verge.io). Remote staff: All staff are hybrid 3/2.

Question: Which critical business systems and platforms are in scope (e.g., Salesforce, IvyTek, Sage Intacct), and how are they currently supported?

Answer: Salesforce / IvyTek / Sage Intacct – Core Integrated Business Applications (IBA). DocuWare Cloud + SharePoint Online – Records and document management. Zendesk – Ticketing and service operations. Enable (TechPG) – Program management and reporting. Supported by internal IT Team & Data/Security Officer; SOC/MSP handles infrastructure monitoring and patching.

Question: What existing monitoring, alerting, and ticketing tools are used (e.g., Zendesk, SolarWinds, Azure Monitor)?

Answer: Ticketing: Zendesk (Service Desk, Change, Procurement). Monitoring: Auvik (network), Adlumin (SOC), Microsoft Defender EDR/MDR. Patch Management: Securin (Qualys + Ivanti). Cloud Monitoring: Azure Monitor and Purview Compliance Portal.

Question: What are the current response and resolution targets or SLAs that NMFA expects to maintain or improve upon?

Answer:

Priority	Response	Resolution	Target
Critical (P1)	15 min	4 hrs	99 % within target
High (P2)	1 hr	8 hrs	95 % within target
Medium (P3)	4 hrs	2 business days	90 %
Low (P4)	1 day	5 business days	85 %

Question: How many internal IT staff currently perform support or NOC functions, and what is their expected role during and post transition?

Answer: Current staff: 5 (IT Manager, System Admin, Network Admin, Support Tech, CTO). Post-transition: Internal team focuses on governance, vendor management, and project oversight; MSP handles Tier 1–2 operations and NOC coverage.

Question: What is the anticipated timeline and critical milestones for transition, go-live, and full operational handover?

Answer:

Phase	Milestone	Target
1 – Discovery	Requirements + Asset Validation	Q1 2026
2 – Pilot NOC	Partial Cutover (IT + Finance)	Q2 2026
3 – Full Go-Live	Org-wide service support	Q3 2026
4 – Optimization	KPI review + SLA tuning	Q4 2026

Question: Are there specific cybersecurity or compliance frameworks (e.g., ISO 27001, NIST, CIS) the MSP must operate under?

Answer: CIS v8.1 – Operational baseline.

NIST SP 800-61 – Incident management.

SOC 2 Type II – Vendor assurance.

ISO 27001 Alignment – Target 2026 through ControlMap.

Microsoft E5 Security Stack used for MDR and compliance enforcement.

Question: Which KPIs and reporting formats are most important to NMFA leadership for ongoing governance and performance review?

Answer:

Mean Time to Respond (MTTR)

Mean Time to Resolve (MTTR)

SLA adherence %

Patch compliance % and vulnerability age

Endpoint protection coverage %

Monthly service dashboard in Power BI (connected to Zendesk and Auvik)

Question: What are the hours of operation for the Service Support Desk?

Answer: Standard: M–F 7 AM – 7 PM MT. After-hours: 24/7 critical incident coverage via SOC/MSP. Hybrid 8×12 + 24×7 critical

---

Question: Are there any onsite support requirements

Answer: Limited to hardware deployments, network maintenance, and executive support. Must be available within 4 hours for critical on-site needs in Santa Fe, NM.

Question: What is the Tier 3 Expert Support expectations?

Answer: Advanced Microsoft 365, Azure, and network engineering.
Root-cause analysis of persistent issues.
Security event investigation and forensic assistance with Adlumin/Securin.
Change management and architecture advisory to Data & Security Officer.

Question: Is obtaining ISO 20000 certification mandatory for the prime contractor, or is it sufficient to simply adhere to its standards?

Answer: Not Mandatory. NMFA does not require ISO 20000 certification at the time of submission. The prime contractor must adhere to ITIL and ISO 20000-aligned service management principles.

Question: If the prime vendor does not possess ISO 20000 certification, can this mandatory requirement be fulfilled through a subcontractor holding the certification?

Answer: A subcontractor's ISO 20000 certification can be used to meet alignment requirements if the subcontractor performs core service desk or NOC operations. The prime contractor remains responsible for overall service delivery quality and compliance.

Question: Can NMFA provide a current network and system architecture diagram (including on-premises, cloud, and hybrid components)?

Answer: NMFA will provide the network and system architecture diagram to the awarded vendor during onboarding. The environment includes a hybrid topology with Verge.io private cloud, Microsoft Azure GCC, and Meraki cloud-managed network devices.

Question: What is the cloud footprint (Azure, AWS, GCP), and how is identity and access managed (e.g., Azure AD, Okta)?

Answer: Cloud Providers: Microsoft Azure GCC (primary) and Verge.io (private cloud DR).
Identity & Access Management: Microsoft Entra ID (Azure AD P2).
Authentication: Conditional Access and MFA enforced through Entra ID, Intune, and Defender.
No AWS, GCP, or Okta environments in use.

Question: Are there any legacy or unsupported systems still in production that require monitoring?

Answer: No unsupported systems are currently in production. Two legacy Windows Server systems

remain online for limited archival purposes and will be decommissioned in 2026.

Question: What endpoint management tools are currently in use (e.g., Intune, SCCM, CrowdStrike, Defender)?

Answer: Primary: Microsoft Intune (MDM/MAM)
Security Stack: Microsoft Defender for Endpoint (EDR/MDR)
Patching: Securin (Qualys + Ivanti)
No SCCM or CrowdStrike in production.

Question: Are there any custom-built or proprietary applications managed internally that the MSP must support?

Answer: NMFA does not develop or host proprietary applications internally.
All business applications are COTS or SaaS, including Salesforce, IvyTek, and Sage Intacct.
The MSP will not be responsible for custom code support but may coordinate integration or access issues.

Question: Are there critical business systems hosted externally (SaaS) that require monitoring or API-level integration?

Answer: Yes – the Integrated Business Applications (IBA) suite includes:
Salesforce – Loan and program management
IvyTek – Lending automation
Sage Intacct – Financial accounting
Enable (TechPG) – Program reporting
The MSP will monitor connectivity, performance, and API health between these systems and others

---

Question: What network monitoring tools are currently used?

Answer: Auvik – Network device and topology monitoring.
Cisco Meraki Cloud Dashboard – Device management and analytics.
Adlumin – SOC and SIEM monitoring platform.
Azure Monitor – Cloud and VM health tracking.

Question: Are there existing monitoring dashboards or event management platforms that should be

retained?

Answer: Existing dashboards exist in Auvik, Adlumin, and Power BI. The incoming MSP should retain and enhance these dashboards for unified visibility.

Question: Should NOC also handle security monitoring (SIEM/SOC) or strict network and system health?

Answer: The NOC will focus on network, system health, and uptime monitoring.
The SOC functions (SIEM, threat analysis, incident response) are managed by Securin and Adlumin.
Coordination between NOC and SOC is expected during security events.

Question: What is the expected alert escalation workflow (e.g., NOC → NMFA → vendor)?

Answer: NOC detects alert → triages severity.
Tier 1 (MSP) responds and documents in Zendesk.
Escalation Path:

- Tier 2 (MSP/NMFA IT)
- Tier 3 (NMFA CTO/Data & Security Officer or external vendor)

Security-related alerts: Routed directly to SOC (Securin/Adlumin).

Question: For service desk operations, what is the expected coverage window (24x7, 8x5, or hybrid)?

Answer: Standard Hours: Monday – Friday, 7:00 AM – 7:00 PM MT. After-Hours: 24×7 coverage for P1 incidents through SOC/MSP.

Question: What security tools and controls are already in place (e.g., EDR/XDR, SIEM, vulnerability management, firewalls, MFA)?

Answer: EDR/XDR: Microsoft Defender for Endpoint (E5)
SIEM: Adlumin
Vulnerability Management: Qualys + Ivanti via Securin SOC
Firewalls: Cisco Meraki MX
MFA: Enforced through Entra ID (P2)
DLP/Compliance: Microsoft Purview
Email Security: Microsoft Exchange and Barracuda

Question: What is the current SIEM solution (if any)? Is integration with Sentinel, Splunk, or other

platforms required?

Answer: Adlumin (current SOC 24×7 platform). Integration with Microsoft Sentinel may be explored in 2026 for enhanced correlation. No Splunk or third-party SIEM is in use currently.

Question: Are there additional compliance mandates (e.g., ISO 27001, CJIS, FedRAMP, SOX) beyond ISO 20000 and SOC 2?

Answer: Required:

CIS Controls v8.1

NIST SP 800-61 (Incident Response)

SOC 2 Type II for vendors

Optional Alignment: ISO 27001 through ControlMap.

No CIS, FedRAMP, or SOX obligations currently.

Question: Will the MSP need to manage endpoint encryption, MFA enforcement, and password policies?

Answer: Endpoint compliance and encryption (BitLocker via Intune). MFA enforcement (Entra ID Conditional Access). Password policy adherence (Microsoft baseline templates)

Question: What APIs or integrations exist between Zendesk and internal systems?

Answer: Microsoft 365 (Teams & Outlook), AssetSonar (asset inventory), DocuWare (contract/document linking), Power BI (KPI reporting), ClickUp (project alignment and IT task tracking). MSP may integrate RMM/NOC tools via API for ticket automation.

Question: Does NMFA expect automation or orchestration (SOAR-like functions) between the NOC and ticketing systems?

Answer: Desired but not required. NMFA encourages automation between Zendesk, Auvik, and Adlumin for real-time alert correlation and incident creation.

Question: What are the preferred log collection and retention mechanisms (e.g., syslog servers, cloud storage)?

Answer: Syslog & API-based log ingestion into Adlumin SIEM.

Retention:

Operational Logs: 90 days

Security Logs: 1 year

Compliance/Forensic Data: 7 years (aligned with retention schedule)

Question: Will NMFA provide technical documentation, inventories, and credentials during the transition period?

Answer: Network diagrams, System inventories**,** SOPs and escalation matrices**,** Credentials under secure transfer**,** Policy documentation (AUP, Incident Response, etc.)

Question: Is there a shadow/support overlap period with existing staff before full handoff?

Answer: Yes — a 30-day shadow period. The MSP will work alongside internal IT and SOC before full operational handoff.

Question: Should the MSP recommend license optimization and consolidation strategies, or only manage existing licenses?

Answer: Yes.

Question: MSP provide executive summaries and trend analyses for NMFA's leadership team?

Answer: Yes — MSP must deliver monthly executive summaries with:

Ticket metrics (MTTR, SLA adherence, backlog)

System uptime and availability

Security posture and patch compliance

Trend analysis and recommendations

Reports are provided via Power BI dashboards and monthly review meetings.

Question: What is the reason for transition to MSP.

Answer: NMFA is seeking to consolidate Tier 1–2 operational support and Network Operations Center (NOC) functions into a single managed service model.

Key pain points driving the change include:

Inconsistent ticket resolution times during peak workloads.

Limited overnight and weekend coverage.

Desire for improved automation, proactive monitoring, and measurable KPI/SLA performance tracking through Power BI dashboards.

Need to free internal IT resources for governance, project delivery, and vendor

management

Question: Quantity and make of networked storage devices (e.g. SAN, NAS)?

Answer: Quantity: (2). Make: Verge.io virtualized storage cluster (replaces traditional SAN/NAS). Function: Provides disaster recovery replication and VM storage

---

Question: Quantity and make of hypervisor hosts? Quantity and OS of virtual servers?

Answer: Quantity: (3) hosts. Make: Verge.io virtual infrastructure platform. Virtual Servers: ~10 total (Windows Server 2019 / 2022). Operating Systems: All Windows-based, no Linux VMs currently in production.

Question: Quantity of physical Linux servers?

Answer: Zero (no physical Linux servers in current scope).

Question: EDR / MDR - Currently have anything in place for endpoint detection. What is it? How many devices are being protected? Cost per device? Are we quoting something for this as well?

Answer: Current Solution

Platform: Microsoft Defender for Endpoint (EDR/MDR).

SOC Oversight: Securin and Adlumin provide 24/7 monitoring, alerting, and remediation assistance.

Quoting Expectation may quote additional MDR/NOC overlay services if offering enhanced 24/7 detection, escalation, or response capabilities that supplement existing Defender + Adlumin/Securin stack. However, duplication of coverage is not required.

Question: How would you like the MSP to escalate issues?

Answer: Escalation Expectations

NMFA follows an ITIL-aligned escalation path using Zendesk as the system of record:

Tier	Responsible Party	Escalation Trigger
Tier 1 – Service Desk (MSP)	Initial triage, password resets, access, endpoint troubleshooting	New tickets
Tier 2 – MSP/NMFA IT	Infrastructure, network, app issues not resolved by Tier 1	After 30 min–2 hrs
Tier 3 – Internal IT/SOC	Security incidents, root-cause, config changes	After Tier 2 review or P1 /P2 incident
Tier 4 – Vendors	Salesforce, IvyTek, Sage Intacct, etc.	As needed through vendor support contracts

All escalations must be documented in Zendesk with ticket status and timestamp.

Question: Is there currently a knowledge base available? If so, which application?

Answer: Knowledge Base

Current Platform: Zendesk Guide

Content Scope: User FAQs, IT Policies, and self-help articles (≈ 75 entries).

Maintenance: Joint between NMFA IT and Communications Team.

Question: Are you open to utilizing the MSP's ITSM? If so, do you envision Co-Manage access will be required for existing/remaining NMFA IT staff? Co-Manage' refers to tenant-specific software licenses to access and manage (ticket) activity directly in ITSM. Please state the number of co-Manage licenses required in such an arrangement.

Answer: MSP ITSM / Co-Manage Access

Preferred: Continue using NMFA's Zendesk ITSM.

Co-Manage Licenses: If the MSP proposes using their own ITSM, NMFA requires 5 co-manage licenses for IT Manager, System Admin, Network Admin, Support Tech, and CTO.

Integration: APIs must sync tickets and SLA metrics back to NMFA's Power BI dashboard.

Question: Do you have your own chatbot? If so, which one, if not, are you open to using MSPs?

Answer: NMFA has Zendesk Chabot

Question: How is IT end-user equipment (laptops, peripherals, smart devices) procured and provisioned for employees? Is the MSP expected to take on this responsibility and/or share this responsibility with NMFA IT staff? Describe the preferred arrangement.

Answer: Procurement & Provisioning of End-User Equipment

Procurement handled jointly by IT and Finance through Zendesk Procurement Workflow.

Provisioning uses Intune Autopilot for Windows devices, BYOD MDM for mobile devices.

MSP is expected to assist with device procurement and provisioning, not own it entirely.

Preferred arrangement:

NMFA IT orders / approves hardware

MSP coordinates imaging with vendor and delivery via Autopilot per standard build policies.