MEMORIAL

UNIVERSITY

MEMORIAL UNIVERSITY OF NEWFOUNDLAND

REQUEST FOR PROPOSALS
FOR

CYBERSERCURITY UPGRADE AND MANAGED SECURITY SERVICES

RFP-039-26 ADDENDUM # 2

Date: August 12, 2026

Purpose of Addendum 2:

MUN CAIR — Cybersecurity RFP

Consolidated Clarifications (Addendum)

Cybersecurity Upgrade and Managed Security Services

This addendum consolidates all bidder questions and CAIR's responses; duplicate questions have been merged.

1. Overarching Guidance

This is a request for proposal. We have given guidance as to the functionality and capabilities we would like to implement, but we are genuinely open to your recommendations on the best solution possible. If we have asked for something you don't feel is required or necessary or cost-prohibitive, please call it out and provide justification/explanation.

This is a new contract. There is no incumbent, and no transition from a prior provider is required.

Protected B alignment means CAIR would like a no-regret path to a future Protected B alignment. Bidders must highlight in their proposal their conformance to Protected B controls and describe high-level how Protected B accreditation could be achieved in future by adding or enabling controls. We wish not to go backwards if it can be avoided. Any component that would require replacement to reach Protected B must be identified as such, with rationale (e.g., cost-prohibitive but easily changed out).

Any component, service, or personnel access located outside Canada, or off the Protected B path, must be declared by the bidder with rationale and is subject to CAIR written approval prior to implementation. An undeclared offshore offering is grounds for disqualification.

Please provide unit or tiered pricing for each component of your offering. The data center is growing; what we have today will most likely change as more users are added or additional computing power is deployed. If you require a minimum baseline of activity, please specify.

2. Procurement & Submission

2.1 Proposal deadline / extension **Can bidders have an extension to submit?**

Response: An extension of three weeks has been granted to all bidders.

2.2 Single vs. multiple award **Will the contract be awarded to a single vendor or multiple vendors?**

Response: We prefer to award to a single Prime Contractor, but are open to splitting scope if no single vendor can meet all requirements. One organization must be designated Prime and remain accountable for integration and delivery.

2.3 Incumbent **Who are the previous incumbents on this project?**

Response: Not applicable, this is a new contract with no incumbent.

2.4 References **May we use U.S. client references, and what evidence demonstrates Protected B experience?**

Response: U.S. client references are acceptable. For Protected B experience, prior assessments, attestations, client references, and control-mapping documentation are all accepted.

2.5 Delivery model **Will work be on-site or remote, and how many facilities are in scope?**

Response: Delivery is remote. There is only one in-scope location 4M406, Clinch Crescent, Medical Faculty. No on-site implementation is anticipated.

2.6 Proposal packaging **Should the technical and financial/commercial proposals be one PDF or two separate attachments (RFP says one ≤15 MB PDF; Appendix A calls the financial proposal "separate")?**

As stated in Proposal Requirements and Content. Please send Technical Proposal and Financial Proposal in two separate files. If your files are greater than 15MB, you may be required to send multiple emails. Please ensure to label them as such i.e (Email 1, Email 2 etc..)

2.7 Appendix A tables **Must bidders reproduce the Appendix A mandatory-requirements tables, or is an equivalent compliance matrix following Appendix A numbering acceptable?**

The Table in appendix a should be completed as shown in open call for bid document.

2.8 Page limit / formatting **Is there a page limit or additional formatting requirement beyond one English-language PDF ≤15 MB, cross-referenced to RFP sections?**

No there is no page limit. However, in regards to size, please see comment above 2.6

2.9 Form of Agreement **Appendix B refers to a Form of Agreement that was not included — will it be issued by addendum?**

There is no actual agreement per se, the open call document in its entirety will form the agreement.

2.10 WorkplaceNL / H&S **Do the WorkplaceNL Certificate of Clearance and contractor health-and-safety requirements apply where services are delivered entirely/primarily remotely with no work on University property?**

Response: Where all services are delivered remotely and no vendor personnel perform work on University property, the WorkplaceNL Certificate of Clearance and contractor health-and-safety documentation are not required. If on-site activity required, this would trigger them.

3. Commercial & Pricing

3.1 Previous spend **What was the previous annual spend on this project?**

Response: Not applicable. No multi-layer security approach is currently in place.

3.2 Budget **What is the annual budget for this contract?**

Response: To be determined based on the solutions proposed. We are seeking the most efficient and effective solution.

3.3 Pricing model **How should pricing be structured given a growing environment?**

Response: Provide unit or tiered pricing for each component. The environment will not remain static and will change. State any minimum baseline of activity you require.

3.4 Contract term & extensions **What is the term, and the number/duration of extension periods after the preferred 3-year contract?**

Response: Preferred term is three years.

With two additional one-year extension periods at CAIR's sole option (3 + 1 + 1) totaling potential 5 year contract.

3.5 Billing & prepayment **Is annual subscription billing acceptable, and would the §2.9 prepayment security requirements apply to multi-year upfront payment?**

Annual subscription upfront billing is acceptable to CAIR. Multi-year upfront prepayment is not. The SOC services should be on a monthly basis or quarterly basis.

3.6 Pricing breakdown **Should pricing be separated into mandatory, optional, and future Protected B roadmap components?**

Response: Yes. Please separate pricing into your proposed (i) mandatory requirements, (ii) proposed optional requirements. Each with unit or tiered pricing. (iii) Future Protected B road map compoments a high level estimate would be appreciated.

3.7 Optional DAM in TCO **Will the optional Data Security Monitoring & Real-Time Audit capabilities be scored and included in Total Cost of Ownership?**

Response: This RFP, since this is genuinely an ask to determine the best overall solution, will be evaluated on best overall protection-per-dollar, judged by overall outcome not specific tools. We are open to suggestions on what the overall capabilities should be.

3.8 TCO evaluation **How will TCO be evaluated where bidders propose materially different architectures, licensing metrics, or optional components?**

Response: Agreed this is the tricky part of an RFP in which many different solutions are available. We will look at overall protection-per-dollar. Unit and tiered pricing will be used to normalize differing licensing metrics and architectures to a common basis for comparison.

4. Current Environment — Volumes

The following consolidates the environment details requested across multiple bidders. All figures reflect the current state; the environment is growing, so provide unit/tiered pricing accordingly.

Users with IT access	Approx. 700 today. Pricing requested for 400–800 (cleanup and growth expected as we move into the new stance).
Peak concurrent users	100–150, expected to grow.
Servers — physical (on-prem)	80
Servers — virtual (OpenStack)	84 VMs
Servers — OpenShift	20
M365 users	0
Sites in scope	One. 4M406, Clinch Crescent, Medical Faculty.
Internet link	1 Gig from campus; bandwidth increase planned.
Endpoints outside data center	Approx 10 laptops.

Network devices / assets monitored	Approx 20.
Cloud workloads / assets	None / not applicable.
IoT, lab, facilities or OT assets	<10.
Identities	10 privileged users; 5 service accounts; no non-human identities.
Applications / service-to-service	Aspera.
Anticipated growth	Unknown at this time — provide unit or tiered pricing. Difficult to predict, expecting significant growth possibly double the users.

5. Current Technology Stack

Existing tooling is to be retained except where noted.

SIEM / SOAR	None. (Telemetry currently behind Arctic Wolf, which belongs to MUN main campus and will be phased out.)
EDR / XDR / NDR	None.
Vulnerability management	None dedicated (handled via MUN Security / Arctic Wolf through MUN). Arctic Wolf will not be continued.
Firewalls	Cisco 3140s.
IDS / IPS	Cisco.
VPN / remote access	Cisco.
Identity & directory services	LDAP, Keycloak.
SSO / MFA	Keycloak.
Privileged access management	Role-based.
Micro-segmentation	None — VLAN segmentation only.
Database activity monitoring	None.
User & entity behaviour analytics	None.
Cloud security / CNAPP	None.
ITSM / ticketing / CMDB	Internal ticketing system developed by CAIR; open to recommendations. API and customization can be provided to fit.
Identity governance	IBM Concert currently being installed; CAIR-operated.

6. HPC Environment

Operating system	Linux.
Cluster management	OpenShift and xCAT.
Workload schedulers	IBM LSF; RTM.
Storage	IBM ESS3500; TS4300 tape backup.
Network	Cisco Ethernet; InfiniBand high-speed storage back-end.

Internal link speeds	1 Gig uplink; internal mix of 1 Gig and 10 Gig; a handful of 100 Gig Ethernet.
Security agents on compute nodes	Permitted — agents may be installed on HPC compute nodes. Future co-lo servers may not provide OS access; price both agent-based and agentless / network-based options for future growth.
Systems that cannot tolerate agents / inspection / automated containment / interruption	None at this time; may exist in future.

7. Protected B Alignment & Scope of Compliance

7.1 Scope of compliance **Is compliance limited to (a) technical/architectural controls, or (b) full Protected B personnel and operational requirements including screening?**

Response: Scope is (a). No government security screening (Reliability Status / Secret) is required at this time, but the staffing model should be able to accommodate Reliability Status screening of relevant personnel in future.

7.2 Data residency (cloud) **The RFP names AWS Canada or Azure Canada — are equivalent Canadian-hosted services from other providers acceptable?**

Response: Yes. Any Canadian-hosted service is acceptable provided it aligns with a future Protected B status. Not limited to AWS or Azure.

7.3 Personnel location **Must SOC analysts, incident responders, and vulnerability-management resources be physically located in Canada, or is Canadian data residency sufficient? Is a hybrid offshore/onshore model acceptable?**

Response: Preference is resourcing aligns with a Protected B path — i.e., could be convertible to full Protected B later if needed. A hybrid offshore/onshore model is acceptable where security requirements are met and any offshore element is declared and approved per the overarching guidance. Can also offer both options if cost benefit is significant.

7.4 Personnel screening **Are federal security clearances or reliability status required for vendor personnel with system/data access?**

Response: Formal Government of Canada security clearance is not required at this time, this is a future state.

For this application we will follow Memorial's research security standard which is 1) verified identity; (2) a Canadian criminal record check (CPIC), completed within the previous six months; (3) employment and education verification covering the preceding five years; and (4) a signed confidentiality/non-disclosure agreement and CAIR data-handling acknowledgement. Memorial University's existing research-security screening process conducted internally by our Research Security Manager.

7.5 Assessment / accreditation during term **Is any formal Protected B assessment, SA&A, TRA, PIA, control validation, or accreditation expected during the contract term?**

Response: The annual cybersecurity risk assessment listed in the RFP applies. Full Protected B assessment is not required in this phase.

7.6 Evidence of experience **What evidence should bidders provide to demonstrate Protected B experience?**

Response: Prior assessments, attestations, client references, and control-mapping documentation are all accepted.

8. Managed Security Services & SOC

8.1 Operating model **Is the intended SOC model fully managed or co-managed, and how are responsibilities split among the bidder, CAIR, and Memorial OCIO beyond the Tier 1–3 escalation model?**

Response: Co-managed. Please propose the most efficient model between your team and CAIR personnel. Memorial University OCIO is informed only by CAIR.

8.2 Dedicated resource **Is the L1/L2 SOC analyst a named, full-time dedicated resource, and is there a residency requirement?**

Response: The resource(s) can be shared, a research security background check is required. Residency must meet a future Protected B path.

8.3 NDR services **NDR requires ongoing tuning and is not always worth the investment — could it be made optional?**

Response: NDR may be treated as an optional service. Please provide your best recommendation based on your experience.

8.4 SLAs **The RFP requires detection, response, containment, uptime, and support SLAs but sets no minimum targets — should bidders propose their standard framework?**

Response: Yes. Bidders should propose their standard SLA framework and service targets.

8.5 Reporting **Beyond the monthly incident metrics, risk-posture trends, and threat-landscape reporting, what frequency, format, and audience are required for executive, operational, compliance, annual risk-assessment, and service-review reports?**

Response: Monthly operational and incident reporting (audience: CAIR team); quarterly service-review reports and meetings (audience: CAIR and Memorial OCIO); an annual cybersecurity risk assessment with an executive summary (audience: CAIR/OCIO leadership); and compliance/ad-hoc reporting as required for high-potential incidents. Bidders can propose enhancements or alterations to cadence and format.

8.6 Legal / breach support **What is the expected scope of bidder support for legal, privacy, regulatory, and breach-reporting obligations associated with incidents?**

Response: The bidder is expected to support incident response including breach identification, containment, forensic evidence preservation, and preparation of breach-notification content, and to coordinate with CAIR and Memorial University teams. Formal regulatory and privacy-reporting obligations remain CAIR/Memorial's responsibility; the bidder supports but does not own them. Bidders should describe their breach-support model and any 24/7 incident-response retainer.

9. Technical Capabilities & Scope

9.1 Endpoint detection tools **What is the expected scope of the "provision of endpoint detection tools"?**

Response: Two distinct needs. (i) Device posture verification at the point of access for a small group of VPN users (~10 maximum); the bulk of users enter via Zero-Trust access (or other as proposed.) (ii) Endpoint detection and response (EDR) for all nodes and servers inside the data center. For HPC, price both agent-based and agentless / network-based options.

9.2 New hardware vs. software **Is new network security hardware required, or may requirements be met with software, virtual appliances, cloud-delivered services, and existing infrastructure?**

Response: Prefer to minimize new hardware. Prefer software, virtual appliances, existing infrastructure, and cloud-delivered services. Recommend hardware only where genuinely necessary.

9.3 Micro-segmentation **Must micro-segmentation be fully implemented at go-live, and what is in scope (assessment, discovery, design, implementation, enforcement, ongoing tuning)?**

Response: A phased implementation roadmap is acceptable, full implementation is not required at go-live. No micro-segmentation technology exists today (VLAN only), so the proponent should include software, licensing, and implementation. Please recommended solution.

9.4 Identity-based segmentation **What is meant by "identity-based segmentation," and which identity systems must it integrate with?**

Response: It applies to a combination of identity types — user vs privileged, device, application, workload, service accounts/principals, and certificates. Integrate with LDAP and Keycloak.

9.5 East-west traffic inspection **What is the scope of east-west inspection — coverage, telemetry sources, retention, encrypted-traffic handling, and detect-only vs. block?**

Response: The capability must block and contain, not detect only. For encrypted-traffic inspection, please provide your recommendation. Relevant speeds are per Section 6. Bidders should propose their recommended approach.

9.6 IAM & MFA responsibilities **Should the bidder provide new IAM/MFA or integrate with existing platforms, and is FIDO2/passwordless required for all users?**

Response: Integrate with CAIR's existing platforms where possible (LDAP, Keycloak). Provide MFA technology. FIDO2/passwordless is required only for privileged, sensitive, or high-risk access not all users.

9.7 Identity governance (IBM Concert) **What are the bidder's responsibilities for integrating with, configuring, or supporting IBM Concert and internal identity-governance systems?**

Response: Integrate only, not configure or support. IBM Concert (CAIR-operated) handles access certification, provisioning/deprovisioning, dormant-account detection, and least-privilege enforcement. CAIR is in the early stages of adoption of Concert, it can be configured to bidders needs.

9.8 Database activity monitoring **Does DAM exist today, and what is the bidder expected to provide?**

Response: No DAM platform exists today. DAM is an optional RFP capability; propose provision, licensing, and deployment as applicable.

9.9 AI-assisted / autonomous operations **May AI-assisted or autonomous security operations be proposed given the AI-training prohibition?**

Response: Yes , provided CAIR data remains within approved Canadian environments, is not used for model training, and all automated actions remain subject to approved governance and response playbooks.

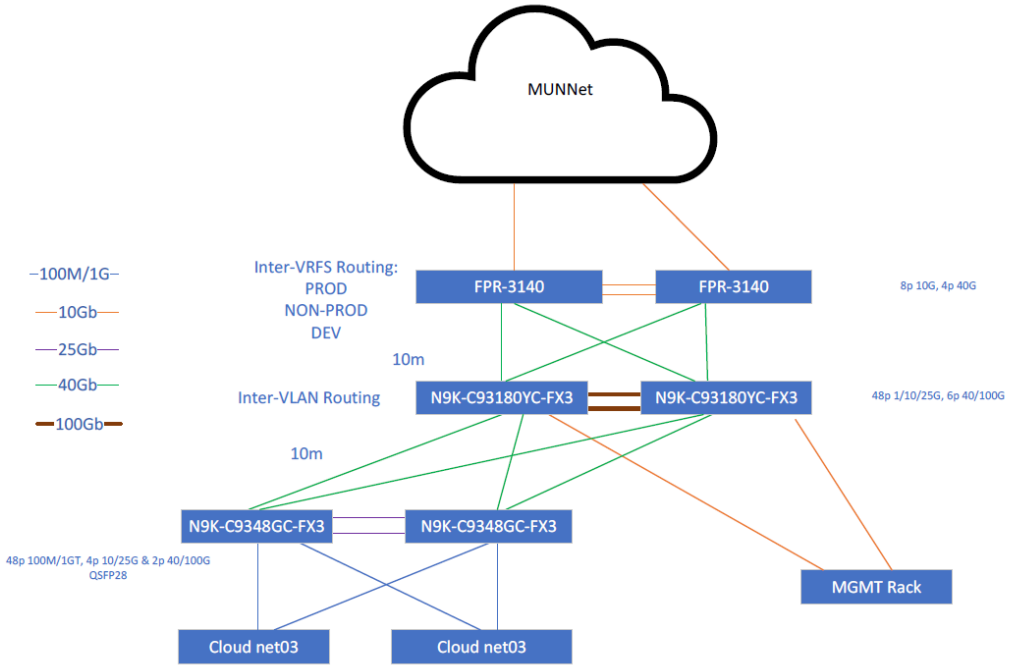
9.10 Log ingestion & retention **What are current average/peak daily log-ingestion volumes or EPS, expected growth, and required searchable/online/archival retention periods?**

Response: Based on Cisco FMC connection-event statistics, the firewall generates approximately 250,000 connection events per day, averaging roughly 3 events per second. Cisco ISE authentication logging is far lower, with a maximum observed volume of approximately 73 events per day (<0.01 EPS). Combined ingestion from these two sources is estimated at approximately 250–500 MB per day. These measurements were collected during the summer period, when research activity and associated network utilization are typically lower; volumes are expected to rise during peak academic and research periods, and while a peak of 20 EPS is estimated for these sources, actual EPS may be higher.

Bidders should treat the figures above as a baseline representing perimeter and authentication telemetry only. They exclude additional infrastructure and application sources which are expected to become the dominant contributors to overall log volume once onboarded, particularly as endpoint and host logging are enabled. Bidders should size for this growth rather than treating the current 250–500 MB per day as a ceiling. For capacity-planning purposes, CAIR anticipates approximately 25–30% growth in the next year driven by expanding research partnerships and service offerings, 50% growth in the next 3 years. Bidders should propose a solution sized for a sustained ingestion rate and state the EPS or GB/day tier their pricing is based on, so that proposals can be compared on a common basis.

Retention targets are: searchable/online approximately 90 days; archival minimum 12 months for logs and alerts; and incident records and forensic artifacts retained at least 24 months, or longer where subject to legal hold. Bidders should confirm how their proposed model can accommodate.

9.11 Existing Network Diagram



10. Technology Ownership & Transition

10.1 Ownership model **For each in-scope capability, should proponents assume CAIR provides the software/infrastructure, the proponent provides it, or a hybrid applies?**

Response: Hybrid. The proponent provides and licenses new capabilities where none exists today (e.g., SIEM/SOAR, EDR/XDR, NDR, vulnerability management, micro-segmentation, and DAM as optional), and integrates with CAIR-owned platforms where they exist (LDAP, Keycloak, IBM Concert, and the internal ticketing system).

10.2 Transition / incumbent **Does an incumbent deliver any in-scope services, and what transition support is expected?**

Response: No incumbent. No transition from a prior provider is required.

MEMORIAL

UNIVERSITY

MEMORIAL UNIVERSITY OF NEWFOUNDLAND

REQUEST FOR PROPOSALS
FOR

CYBERSERCURITY
UPGRADE AND MANAGED
SECURITY SERVICES

RFP-039-26

ADDENDUM # 1

Date July 30, 2026

Purpose of Addendum 1:

Deadline for receipt of bids has been revised. The new tender closing date is September 10, 2026, at 10:00AM (NST) New Access code: 2774 136 2304