REQUEST FOR PROPOSALS

Cybersecurity & Threat Intelligence Consultant

Issuing Organization: Chicago Quantum Exchange (CQE), The University of Chicago — Lead Organization, AQtivate Component Project of the Bloch Quantum Tech Hub

RFP Issue Date: November 13, 2026

Proposal Due Date: December 11, 2026

Point of Contact and Submission Mechanism: Matthew Zajac, Director of Operations and Strategic Engagement, zajacm1@uchicago.edu

1. Introduction & Background

The Chicago Quantum Exchange (CQE) at The University of Chicago is the lead organization for AQtivate, a component project of The Bloch Quantum, a tech hub designated by the U.S. Economic Development Administration (EDA) serving Illinois, Wisconsin, and Indiana. The Bloch's mission is to establish the region as the nation's leading hub for manufacturing quantum technologies.

AQtivate supports and scales The Bloch's component projects, including through security and risk mitigation. The goal of this activity is to safeguard the region's quantum manufacturing ecosystem in alignment with the NIST Cybersecurity Framework (CSF) 2.0.

CQE, on behalf of AQtivate and The Bloch, is seeking a qualified cybersecurity and threat intelligence firm to serve as the program's security consultant. The consultant will develop the frameworks that will guide The Bloch's cybersecurity risk management and lead audits of the ecosystem's cybersecurity capabilities and risk posture.

2. Purpose of This RFP

Through this RFP, The Bloch intends to select a single cybersecurity and threat intelligence consulting firm to:

- Develop a cybersecurity risk-assessment framework and methodology for The Bloch/AQtivate, aligned with NIST CSF 2.0;
- Lead a launch audit establishing a baseline of The Bloch firms' cybersecurity capabilities, vulnerabilities, and risks; and
- Lead annual follow-up audits using that framework, tracking risk reduction and capability maturity over time.

This is an initial, targeted engagement scoped to the current available budget. It is distinct from, and precedes, the broader ecosystem-wide security assessment and training program described in AQtivate's, which extends into remediation and incident response. The Bloch anticipates that the framework and processes developed under this contract will inform and scale into that broader program as additional funding is secured in later program years.

3. Scope of Work

3.1 Cybersecurity Framework Development

- Design a risk-assessment and audit methodology aligned with NIST CSF 2.0, tailored to The Bloch/AQtivate's organizational structure, data infrastructure, intellectual property considerations, and partner network.
- Define risk categories, scoring criteria, and reporting templates that The Bloch can apply to its Risk Mitigation Plan initially, and then consistently year over year.
- Recommend baseline security policies, training content, and compliance metrics appropriate to a multi-institution, federally funded consortium.

3.2 Launch Audit

- Conduct a comprehensive baseline audit of select Bloch quantum or manufacturing firms' cybersecurity capabilities, systems, and practices using the framework developed above.
- Identify and rate vulnerabilities and risks, including those related to data infrastructure, IP protection, and third-party/partner access.
- Deliver a written report of findings with prioritized, actionable remediation recommendations.
- Present findings to the Regional Innovation Officer (RIO) and the Security Advisory Council.

3.3 Annual Audits

- Re-assess Bloch quantum or manufacturing firms' cybersecurity posture annually against the established framework for the duration of the contract.
- Track year-over-year progress on remediation and risk reduction.
- Update the framework and reporting templates as threats, technology, or organizational structure evolve.
- Deliver an annual written report and briefing to the RIO and Security Advisory Council.

3.4 Advisory Support

- Provide light-touch advisory availability between audits to answer questions as remediation steps are implemented.
- Flag any urgent or emerging risks identified during the engagement outside the standard audit cycle.

Out of scope for this contract: incident response/remediation execution (beyond advisory recommendations)

4. Deliverables & Schedule

The table below summarizes expected deliverables and target dates. Specific dates will be finalized with the selected consultant at contract execution.

Milestone	Description	Target Date
Contract execution	Consultant selected and contract finalized	January 2027
Kickoff meeting	Orientation with Bloch staff and Security Advisory Council to draft Risk Mitigation Plan	January 2027
Cybersecurity Framework	Deliver written risk-assessment framework and methodology aligned with NIST Cybersecurity Framework 2.0, tailored to The Bloch/AQtivate	April 2027

Milestone	Description	Target Date
Launch Audit	Complete baseline cybersecurity and risk audit; deliver findings report with risk ratings and prioritized remediation recommendations	June 2027
Remediation advisory	Light-touch advisory support as findings are addressed; update Security Advisory Council	Ongoing through contract year
Annual Audit (recurring)	Re-assess against the framework; deliver updated report and year-over-year trend summary; present findings to RIO and Security Advisory Council	Annually, each contract year thereafter

5. Period of Performance & Budget

Available Budget: $30,000 in initial year

Contract Type: Firm-fixed price, annual

Initial Term: One year from contract execution (target: Q1 2027 – Q1 2028)

Renewal: Additional one-year terms by mutual agreement, contingent on funding availability, satisfactory performance, and continued need, for a total potential period through August 31, 2031 (the end of The Bloch's award period). **The Bloch expects future contract period budgets to be significantly larger, with access to additional funds and commitments**.

Proposals should reflect a cost-effective, efficiently scoped approach within the $30,000 initial budget. Offerors are encouraged to describe how they would prioritize effort across framework development, the launch audit, and ongoing annual audits within this budget, and to note any assumptions (e.g., level of effort in hours, on-site vs. remote work, tooling costs) underlying their cost proposal.

6. Consultant Qualifications

CQE is seeking a firm with:

- Demonstrated experience conducting cybersecurity risk assessments and audits aligned with NIST CSF 2.0 or comparable frameworks;
- A track record advising research consortia, public-private partnerships, and firms (experience in emerging technology, national-security-adjacent, or export-controlled environments is a plus);
- Threat intelligence capabilities relevant to intellectual property protection and nation-state or industrial espionage risk;
- Key personnel holding relevant industry certifications (e.g., CISSP, CISM, GIAC, or equivalent);
- Familiarity with, or willingness to coordinate alongside, federal partners such as CISA and the FBI, and awareness of export-control considerations (e.g., ITAR/EAR) relevant to quantum technology; and
- Ability to deliver a right-sized engagement within a limited annual budget, with clear, actionable reporting for a non-technical governance audience (the Security Advisory Council and RIO).

7. Proposal Requirements

Interested firms should submit a proposal (PDF preferred, not to exceed 5 pages excluding resumes and cost proposal) via email to zajacm1@uchicago.edu that includes:

1. Cover letter identifying the firm, primary contact, and a brief statement of interest.
2. Firm overview and relevant experience, including any examples of comparable engagements.
3. Proposed approach and methodology for the framework, launch audit, and annual audit cycle.
4. Key personnel and qualifications, including who will be assigned to this engagement and their role.
5. Work plan and timeline mapped to the schedule in Section 4.
6. Cost proposal, itemized to show how the initial budget of $30,000 could be allocated between the activities in Section 3 (including how many firm audits can be performed), and what reasonable higher budgets in future years could achieve.
7. Disclosure of any actual or potential conflicts of interest.

8. Evaluation Criteria

Proposals will be evaluated by The Bloch using the criteria below.

Criterion	What we're looking for
Technical approach & methodology	Soundness of proposed framework approach and audit methodology; alignment with NIST CSF 2.0
Relevant experience & past performance	Track record with comparable organizations (research consortia, universities, public-private partnerships, or emerging-tech/critical-technology environments)
Key personnel qualifications	Certifications (e.g., CISSP, CISM, GIAC) and hands-on experience of staff assigned to this engagement
Cost & value	Reasonableness and clarity of cost proposal within the available budget

9. Submission Instructions & Key Dates

Action	Date
RFP issued	November 13, 2026
Deadline for written questions	November 30, 2026
Answers to questions posted	December 4, 2026
Proposals due	December 11, 2026, 5:00 PM Central Time
Anticipated award / contract execution	January 2027
Anticipated engagement start	January 2027

Thank you for your interest in supporting The Bloch's mission to secure and grow the nation's quantum manufacturing ecosystem.