



REQUEST FOR PROPOSAL (RFP)

FOR

ROCHESTER INSTITUTE OF TECHNOLOGY

OPENSSL VULNERABILITY TESTING SERVICES

PROPOSAL IS DUE BY OCTOBER 15, 2026 AT 10:00 A.M.

SEND PROPOSAL RESPONSES TO:

PROCUREMENT SERVICES OFFICE

RICHARD ROESER

PURCHASING MANAGER

rxrpur@rit.edu

RIT INTERNAL CLIENT/ DEPARTMENT

DR. BILLY BRUMLEY

RESEARCH DIRECTOR, ESL GLOBAL CYBERSECURITY INSTITUTE (GCI)

bbbics@rit.edu



TABLE OF CONTENTS

1.	INTRODUCTION	3
2.	RIT BACKGROUND INFORMATION	3
3.	RFP PROJECT SCHEDULE	3
4.	CONTRACT AWARD IN BEST INTEREST	4
5.	NON-DISCRIMINATION COMPLIANCE	4
6.	CONFIDENTIALITY	4
7.	INSTRUCTIONS FOR SUBMITTAL	5
8.	EVALUATION CRITERIA	5
	A: Pricing.....	6
	B: Operating Requirements.....	6
	C: Quality Metric/Performance Metrics	6
	D: Evidence of Business Performance	6
	E: Sustainability (Green Strategy)	7
	F: Terms and Conditions	7
9.	GLOSSARY OF TERMS.....	8
10.	ATTACHMENTS	8



1. INTRODUCTION

Rochester Institute of Technology (RIT/University) is soliciting competitive written proposals for OpenSSL Vulnerability Research as detailed in Section 8 and Attachment A. [All work must be conducted remotely. RIT cannot and will not guarantee any purchase volume under any contract resulting from this RFP.

RIT aims to minimize all sources of supply and agrees to use the Provider as the primary source for the agreed-upon Vulnerability Research. While every effort will be made to purchase from the successful Provider, this should not be interpreted as an "exclusive" agreement for all of RIT's requirements for such services. The Provider must also agree to deliver comprehensive solutions to meet RIT's total requirements and reduce instances where RIT must seek alternative sources.

2. RIT BACKGROUND INFORMATION

RIT, founded in 1829 as The Rochester Athenaeum, has grown to become one of the nation's largest private universities. RIT is a not-for-profit, privately endowed, co-educational institution composed of nine colleges, emphasizing career education and experiential learning. The university occupies 1,300 acres in suburban Rochester, NY, on Jefferson Road in the Town of Henrietta.

The current enrollment on the Henrietta campus is 19,718 undergraduate and graduate students from all 50 states and more than 100 nations, supported by 3,974 faculty and staff. RIT-owned and operated residence halls and apartments house more than 7,000 students during the academic year.

3. RFP PROJECT SCHEDULE

1. Request for Proposal Issued	September 15, 2026
2. Supplier request for Pre-proposal questions (if needed)	September 21, 2026
3. Proposal Due Date	October 15, 2026
4. Presentations / post-proposal meetings if requested by RIT	October 15-18, 2026
5. Contract Awarded (tentative)	October 19, 2026
6. Contract Start Date (tentative)	October 26, 2026
7. Other critical deliverables if needed	[TBD]



4. CONTRACT AWARD IN BEST INTEREST

RIT reserves the right to accept or reject proposals on each item separately or as a whole, to reject any or all proposals without penalty, to waive any informalities or irregularities, and to contract in the best interests of the University to obtain service requirements that best meet RIT's needs.

5. NON-DISCRIMINATION COMPLIANCE

RIT neither affiliates with nor grants recognition to any individual, contractor, or organization, on or off campus, with policies that discriminate on the basis of age, citizenship, color, creed, culture (including deaf culture), disabilities, gender, marital status, national origin, political affiliation or preference, race, sexual orientation, gender identity, or gender expression, as defined by applicable laws and regulations. The Provider agrees to comply with all federal, state, and local regulations.

Contractor and/or subcontractor shall abide by the requirements of [41 CFR 60-741.5\(a\)](#). This regulation prohibits discrimination against qualified individuals on the basis of disability.

Contractor and/or subcontractor shall abide by the requirements of [41 CFR 60-300.5\(a\)](#). This regulation prohibits discrimination against qualified protected veterans.

6. CONFIDENTIALITY

If, in the course of receiving information from RIT to respond to the RFP, the Provider receives proprietary information related to RIT's business, operations, equipment, or products, the Provider will retain all such information in confidence and will not disclose it, except to its own employees and RIT's employees as necessary for the performance of responding to the RFP. However, this will not prevent the Provider from disclosing any information once it becomes available to the general public through a printed publication, or any information that was already in the Provider's possession at the time it was acquired from RIT, or any information furnished to the Provider by a third party. The Provider shall protect confidential information against unauthorized disclosure using the same degree of care, but no less than a reasonable degree of care, as the Provider uses to protect its own confidential information of a similar nature. The Provider will ensure that each employee or subcontractor agrees to similar confidentiality requirements.



7. INSTRUCTIONS FOR SUBMITTAL

Provider is expected to submit a comprehensive Statement of Work that addresses the project requirements and timeline defined in Attachment A. Supplemental artifacts can be submitted to address issues such as qualifications and references, however all requirements in Attachment A must be addressed.

It is mandatory to submit one electronic version of the response via email, following the proposal outline and date requirements, along with a detailed statement of any exceptions to any part of the request (referencing the specific sections involved). Each section of the Evaluation Criteria (Heading 8) must be individually addressed and fully detailed.

1. Without exception all forms of requested proposal must be e-mailed to rxrpur@rit.edu on or before 10:00 am, October 15, 2026
2. Refer requests for additional information or clarification of requirements to:

Richard Roeser
Purchasing Manager
rxrpur@rit.edu

and

Dr. Billy Brumley
Research Director, ESL Global Cybersecurity Institute (GCI)
bbbics@rit.edu

8. EVALUATION CRITERIA

Proposals will be evaluated in accordance with the following bid submission requirements listed in order of relative importance:

A: Pricing

B: Operating Requirements



- C: Quality and Performance Metrics**
- D: Evidence of Business Performance**
- E: Sustainability (Green Strategy)**
- F: Terms and Conditions**

A: Pricing

Provide a detailed breakdown of how the solution will be priced (hourly rates, flat fee, itemized list price, discount structure, net price). Include detailed information regarding precisely what services, features and support are provided, total costs per day and hour (across resources if there are different rates for different skills, e.g., tester, project manager), and list any ancillary costs. If different pricing options exist, please detail how each might be apply to RIT. If the engagement runs longer than estimated, please detail how change orders are handled and what is the rate for additional engagement time (per day and per hour).

B: Operating Requirements

Service Provider must clearly document the proposed approach and methodology it will utilize to perform the required services described in Attachment A. It is acceptable to use a separate document to respond to this section, however all required services must be included and be in the same order as shown in Attachment A. Responses that do not meet these criteria or are incomplete will be rejected by RIT, and Provider will not be afforded an opportunity to submit a second proposal.

C: Quality Metric/Performance Metrics

The Service Provider must demonstrate that they have the experience and qualification as outlined in Attachment A.

D: Evidence of Business Performance

References

Responses must include at least three (3) customer references or evidence of similar projects.



Account Manager and Contractor Support Personnel

Responses must clearly describe how account management for RIT will be handled if the Provider's proposal is accepted. Clearly define the roles of all personnel who will be involved in the project and provide qualifications for each.

Competitive Advantage

Provider should clearly describe the expertise or experience they can provide that elevates them above other respondents.

E: Sustainability (Green Strategy)

Sustainability:

Please outline your sustainability efforts considering the following information. RIT recognizes that sustainability is a concept that seeks to provide the best outcomes for human and natural environments by meeting the needs of the present generation without compromising the ability of future generations to meet their needs. Whenever possible the University attempts to foster sustainability. Include sourcing products that can be recycled or are biodegradable and that contain less toxic and hazardous chemicals and additives; source reduction; and solid waste reduction as well as purchasing local goods that are grown in environmentally sound ways or buying products through systems that produce the least number of environmental pollutants. The University desires that the Provider foster sustainability and partner with the University in the expanding areas of sustainability.

F: Terms and Conditions

Purchase Order Terms and Conditions:

The Contractor will accept and adhere to RIT Purchase Order Terms and Conditions as outlined on the Procurement Services website at:

<http://www.rit.edu/procurement/policies/terms.html>

RIT General Conditions of the Contract for Construction:

The Provider will accept and adhere to the RIT General Conditions of the Contract for Construction outlined in the Facilities Management Services website at:



[Construction Documents | Procurement Services | RIT](#)

RIT Parking Regulations & Restrictions:

The Provider will accept and adhere to the RIT Parking Regulations & Restrictions as outlined on the Parking website at:

[Rules & Regulations | Parking and Transportation Services | RIT](#)

RIT Parking Passes for Vendors & Contractors

The Provider will accept and adhere to the RIT Parking Guidelines for Vendors & Contractors as outlined on the parking website at:

[Vendors & Contractors | Parking and Transportation Services | RIT](#)

Payment Works Vendor Registration:

RIT has partnered with Payment Works to provide a secure supplier onboarding portal. RIT joins many other higher education institutions that have also implemented Payment Works to automate the vendor management processes, protect against business payment fraud, and ensure regulatory compliance. This solution cuts down on the use of paper forms and manual circulation of supplier information. The use of the portal is free of cost to our suppliers and will provide a secure method for providing new or updated information and will give additional visibility into the payment process.

The successful bidder will be **required** to onboard through this Payment Works system **PRIOR** to receiving payments.

For more information on Payment Works, please visit:

[Payment Works Onboarding | Procurement Services | RIT](#)

9. GLOSSARY OF TERMS

N/A

10. ATTACHMENTS

Please make sure to attach these forms to your RFP submission:

- a. Attachment A: Project Statement & Provider Requirements



Attachment A: Project Statement & Provider Requirements

Project Overview:

The bidder must provide professional services to conduct vulnerability research to find and fix vulnerabilities in OpenSSL.

Core Responsibilities:

Audit and Discovery: Conduct audits across the Provider, Primitive, and Protocol layers using a combination of static analysis, dynamic fuzzing, and side-channel verification.

Tooling Development: Develop shims to bridge OpenSSL APIs with existing benchmarking and verification infrastructures (e.g., SUPERCOP).

Vulnerability Validation: Confirm the exploitability of discovered flaws, particularly those involving timing leaks or memory safety in complex parsing logic.

Coordinated Disclosure: Work closely with OpenSSL and the relevant stakeholders to ensure coordinated security disclosure and patch integration.

Regulatory Alignment: Ensure that all proposed remediations (patches/architectural changes) are compatible with FIPS 140-3 requirements.

Open Source Contribution: All methodologies and developed testing tools must be released as open-source software.

The Bidder must perform a systematic vulnerability research project targeting OpenSSL, focusing on three core domains:

Domain 1: Providers: Systematic audit of the OpenSSL 3.0+ provider API and the EVP abstraction layer. Analysis of the FIPS boundary, including parameter validation and error handling. Investigation of memory handling errors in provider context management. Implementation of interface fuzzing and differential provider testing.

Domain 2: Primitives: Security analysis of main NIST Post-Quantum Cryptography (PQC) standards: ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205). Verification of constant-time execution to prevent timing side-channel attacks. Integration of OpenSSL



primitives into the SUPERCOP benchmarking framework and use of TIMECOP for dynamic analysis.

Domain 3: Protocols: Security analysis of the QUIC and HPKE (Hybrid Public Key Encryption) protocol implementations. Audit of protocol state machines to identify memory-safety issues. Analysis of X.509 certificate handling and hybrid signature schemes (combining classical and PQC algorithms) for parsing errors and buffer management vulnerabilities.

Bidder Qualifications:

RIT will consider bids submitted from all providers, given preference to bidders who demonstrate expertise in the one or more of the following fields:

- Specialized cryptography consultancy companies with knowledge of NIST cryptography standards and FIPS validation requirements.
- Cryptographic vulnerability research specialists with a proven CVE track record of identifying and mitigating vulnerabilities in cryptographic software.
- Independent cryptography experts with documented history of contributions to open-source software and a proven peer-reviewed publication track record.

Minimum Experience:

Work Experience: 10+ years of research experience or related work experience.

Education: Must hold a PhD (or PhD equivalent) in Computer Science, Computer Engineering, Electrical Engineering, or Mathematics.

Publication track record: Bidders should provide evidence of a peer-reviewed publication track record, specifically related to cryptography and data security.

Security Track Record: Bidders must provide evidence of a CVE track record, specifically related to widely-used cryptographic libraries.

Advanced Tooling Proficiency: Demonstrated expertise in static analysis tools (e.g., CodeQL, Semgrep), formal methods (e.g., CBMC, Frama-C) for software verification, and dynamic analysis tools (e.g., TIMECOP, SUPERCOP).



Knowledge of NIST standards and FIPS validation: Proven expertise in NIST cryptographic standards and a deep understanding of the FIPS 140-3 validation lifecycle, including the implications of architectural changes on module certification.

Project Deliverables:

Project timeline: 24 months.

Key Deliverables:

Completion of the project, and subsequent payment, shall be contingent on clear delivery of the following:

1. Initial audit of OpenSSL providers, primitives, and protocols
2. Providers: Provider API mapping
3. Primitives: Integration of SUPERCOP and TIMECOP
4. Protocols: Pattern library for HPKE and QUIC
5. Providers: Analysis results
6. Primitives: Analysis results
7. Protocols: Analysis results
8. Vulnerability disclosure

Project Milestones:

- Milestone 1: (August 2027):
 - Completion of the first full audit round
 - Filing of initial findings with the OpenSSL Security Team
 - “Go/No-Go” decision point for effort reallocation.
- Final Milestone (July 2028):
 - At least one accepted, stable OpenSSL release addressing identified vulnerabilities
 - Release of open-source tooling; and presentation of results at the OpenSSL Conference.

Evaluation Criteria:

Proposals will be evaluated using the following scoring methodology:



Technical Expertise (60%): PhD-level expertise, CVE track record, Peer-reviewed publication track record, NIST/FIPS knowledge

Tooling Proficiency (20%): static and dynamic analysis tools, formal methods

Execution Capability (20%): immediate availability and ability to execute an accelerated schedule

Compliance Requirements:

- **Open Source Commitment:** Bidders must agree that all developed tooling and methodologies will be released under an open-source license.
- **Contributor Agreements:** Bidders must agree to sign and file a Contributor License Agreement (CLA) with OpenSSL, and abide by it.
- **Stakeholder Engagement:** Bidders must have demonstrated experience in interacting with a diverse set of stakeholders (industry, academia, government).
- **Regulatory Compliance:** All work must propose FIPS-compliant code changes, so that OpenSSL's FIPS 140-3 validation status can be maintained.