Request for Proposals
Cybersecurity Assessment

Issue Date:

Monday, November 9, 2026

Proposals Due:

Monday, December 7, 2026 by 5:00 P.M.

Pennsylvania Intergovernmental Cooperation Authority

1500 Walnut Street / 16th Floor / Philadelphia, PA / (215) 561-9160

www.picapa.org

Notice: PICA does not discriminate on the basis of race, color, sexual orientation, religion, ancestry, ethnicity, sex, gender identity, age, national origin, familial status, or disability. PICA does not discriminate against faith-based organizations.

Note: This publication was generated with support from ChatGPT. In accordance with the PICA policy on generative AI, all content was reviewed by PICA Staff prior to publication.

Contents

Section 1: General Information 2
Section 2: Project Summary 3
A. Project Information 3
B. Statement of Work 4
C. Reporting and Deliverables: 4
D. Unique Capabilities or Qualities 5
E. Specific Proposal Instructions 6
Section 3. Evaluation and Award Criteria 7
A. Evaluation Criteria 7
B. PICA Rights 7
Section 4. Disclosure of Litigation; Disclosure of Administrative Proceedings 8
Section 5. Nondiscrimination / Sexual Harassment Clause 8

Section 1: General Information

This Request for Proposals (RFP) provides information to enable qualified firms to submit a proposal to conduct a cybersecurity assessment for the Pennsylvania Intergovernmental Cooperation Authority (PICA).

Submit all questions, inquiries, and requests for information concerning this RFP by 5:00 P.M. local time, **Monday, November 23, 2026** in writing via email to:

Marisa Waxman

Executive Director

pica@picapa.org

Marisa Waxman will be the sole point of contact for this RFP. To receive consideration, proposals must be received by 5:00 P.M. local time, **Monday, December 7, 2026** via email to pica@picapa.org. PICA will not be liable for any cost related to the development, preparation, transmittal, or presentation of any proposal submitted in response to this RFP. The last day for questions regarding this RFP will be **Monday, November 23, 2026**. Email any questions to pica@picapa.org.

The submission of a proposal shall be considered evidence that the proposer has read and agrees to the terms and conditions specified in this RFP.

Any modifications or changes made to this RFP will be made in writing in the form of an addendum issued by PICA. Oral communications from PICA staff or others concerning this request for proposals shall not be binding on PICA and shall not in any way be considered as a commitment by PICA.

In addition to a written proposal, prospective firms may be required to give oral presentation or participate in interviews with PICA. All materials submitted for the RFP shall become the property of PICA.

Section 2: Project Summary

A. Project Information

The Pennsylvania Intergovernmental Cooperation Authority (PICA) is an independent authority of the Commonwealth of Pennsylvania, created to provide fiscal oversight for the City of Philadelphia. PICA is a small organization (4 staff, $1.7 million annual budget) that relies on an outside IT services management firm to help us manage our digital infrastructure and services. We primarily use our digital spaces for collaboration on Office Suite, Adobe software, and QuickBooks. We also maintain a digital archive of public finance documents that date back to the early 1990s. Most importantly, we are responsible for transferring tax revenues from the Commonwealth of Pennsylvania to the City of Philadelphia on a weekly basis (roughly $800 million per year).

PICA was initially expected to sunset in 2023, before being reauthorized until at least 2047. To ensure ongoing reliability of our work over the coming decades, we want to ensure our approach to cybersecurity is set up to carry us into the future. We are seeking a service provider to assess the cybersecurity of our current environment and highlight the gaps we would need to close and steps we would need to take to adopt and maintain practices in line with the NIST Cybersecurity Framework 2.0. PICA aims to start the engagement no later than January 26, 2027 and all work should be submitted and accepted by June 15, 2027.

Background of PICA

PICA is charged with collaborating with the City of Philadelphia to maintain and enhance its fiscal condition. PICA was created in 1991 to assist the City of Philadelphia (City) in overcoming a severe financial crisis. PICA is a political subdivision of the Commonwealth of Pennsylvania (Commonwealth) constituting a public instrumentality. PICA is governed by a five-member board with one

member appointed by the Governor, and the other members appointed by majority and minority leaders of the Pennsylvania House and Senate. PICA's Executive Director is appointed by the Board, and the PICA staff currently consists of four employees. PICA will be in operation at least until 2047.

B. Statement of Work

The selected consultant shall conduct an assessment that should address, at a minimum:

- Cybersecurity governance, accountability, and risk management.
- Existing policies, procedures, documentation, and staff practices, or lack thereof.
- Network, endpoint, identity, access, email, cloud, backup, and data-security controls.
- Third-party vendors, managed IT services, software providers, and supply chain risks.
- Asset inventories, data classification, records retention, and protection of sensitive information.
- Vulnerability management, system configuration, patching, monitoring, and logging.
- Security and continuity risks associated with mission-critical operations, including financial transfers, financial system access and authorization, and dependencies on external service providers.
- Incident response, business continuity, disaster recovery, and backup restoration.
- Security awareness and staff training.
- Alignment with the six NIST CSF 2.0 functions: Govern, Identify, Protect, Detect, Respond, and Recover.

The assessment should incorporate review of relevant documentation, interviews with PICA staff and service providers, and examination of available technical configurations and supporting evidence, as appropriate. Respondents should identify the extent to which their assessment will independently validate reported cybersecurity practices and controls.

Proposals should clearly state whether technical testing, such as vulnerability scanning, penetration testing, phishing simulations, or backup-recovery testing are included in the proposal or would be optional additional services.

C. Reporting and Deliverables:

1. Work Plan and Methodology
2. Monthly Project Updates

3. Draft Report
4. Final Report
    a. The final report should contain:
        i. Current-state cybersecurity profile and summary of existing strengths.
        ii. Gap assessment comparing current and target cybersecurity practices against applicable NIST CSF 2.0 categories and subcategories, identifying deficiencies, associated risks, and opportunities for improvement.
        iii. Risk-ranked findings identifying likelihood, potential impact, and urgency.
        iv. Recommended target cybersecurity profile appropriate for PICA.
        v. Prioritized remediation roadmap distinguishing:
            1. Immediate corrective actions.
            2. Near-term actions achievable within approximately one year.
            3. Long-term program, policy, staffing, and technology improvements.
        vi. For each significant recommended action included in the roadmap, identification of the relative priority, estimated implementation timeframe, responsible party (PICA staff, IT service provider, or other), approximate implementation and ongoing costs, and any significant dependencies.
        vii. Identification of recommended policies, procedures, technical investments, and follow-up testing.
        viii. Executive summary of the assessment's principal findings, highest-priority risks, and recommended actions, suitable for organizational planning and Board review.
5. Final Presentation
    a. A presentation of findings and recommendations to PICA and, if requested by the Board, the PICA Board of Directors.

D. Unique Capabilities or Qualities

PICA seeks a consultant or multidisciplinary consultant team that demonstrates substantial experience in the following areas:

- Conducting NIST CSF 2.0 assessments.
- Working with small public agencies, governmental entities, or similarly sized organizations.
- Translating technical findings into practical, risk-based recommendations.

- Independence from vendors whose products or services may be recommended.
- Providing and implementing a clear methodology for protecting confidential information collected during the engagement.

E. Specific Proposal Instructions

Proposals should be prepared simply and economically, providing a straightforward, concise description of capabilities to satisfy the requirements of the RFP.

Respondents are required to submit the following items for the proposal to be considered complete:

1. A cover letter or sheet, including all responding entity contact information, electronically signed by an authorized representative of the submitting entity.
2. A written narrative statement, including:
    a. Unique capabilities or qualities of the respondent;
    b. A record of providing satisfactory services; and
    c. Experience working with clients in government.
3. A statement describing respondent's approach to diversity, equity, and inclusion.
4. A description of the individuals who would be in charge of the project, including their titles and experience with similar entities and projects.
5. A list of references and associated contact information for clients that have received similar services.
6. A description of the firm rendering the proposal, including at a minimum:
    a. Whether the firm is national, regional, or local;
    b. Whether the fir is registered as a woman, minority, or disabled-owned business with the City of Philadelphia or Commonwealth of Pennsylvania;
    c. The number of employees in the firm; and
    d. A commercial activity license and Business Income and Receipts Tax (BIRT) account number issued by the City of Philadelphia.
7. A proposed plan, scope, and timeline for the completion of requested services.
8. A budget including:
    a. An estimate of the costs for requested services
    b. A proposed budget and payment structure (ex. hourly billing, per deliverable)
    c. A not-to-exceed amount for the entirety of the project.

Section 3. Evaluation and Award Criteria

A. Evaluation Criteria

PICA shall evaluate proposals using the following criteria:

1. Experience, expertise, and capability of respondent in providing the requested service to PICA or other similar entities. Particular attention will be given to the size, experience, expertise, capability, and reputation of the firm proposing services related to cybersecurity assessment and framework evaluation.
2. Specific plans for diverse, equitable, and inclusive provision of services;
3. Cost estimates for the work to be provided;
4. Demonstrated ability to complete work in a timely manner;
5. References from other clients; and
6. Completeness of proposal and satisfaction of requirements and specifications set forth herein.

B. PICA Rights

PICA reserves and may exercise the following rights and options with respect to this selection process:

1. To reject any and all proposals and reissue the RFP at any time prior to the execution of a final contract.
2. To supplement, amend, or otherwise modify this RFP at any time prior to selection of one or more proposers for negotiation and to cancel this RFP with or without issuing another RFP with no liability to any potential respondent.
3. To negotiate, accept, or reject any or all of the items in any proposal and award the contract in whole or in part, if it is deemed in PICA's best interest to do so.
4. To reject the proposal of a proposer that, in PICA's sole judgement, has been delinquent or unfaithful in the performance of any contract with the City of Philadelphia or Commonwealth of Pennsylvania, is financially or technically incapable, or is otherwise not a responsible proposer.
5. To waive any minor informality, defect, or deviation from this RFP that is not material to the proposal.
6. To request that some or all of the proposers clarify, modify, or supplement proposals.
7. To request to inspect projects referenced in the proposer's proposal.
8. To conduct investigations with respect to the qualifications of each proposer and contact references.

9. To require the selected proposer to enter into a written contract with PICA that includes all requirements of law applicable to contracts with an agency of the Commonwealth, including the Nondiscrimination/Sexual Harassment Clause described in Section 5 of this RFP, and indemnification of PICA by the proposer, rights of PICA to terminate such contract, and insurance requirements applicable to the proposer.

Section 4. Disclosure of Litigation; Disclosure of Administrative Proceedings

For the five-year period preceding November 1, 2026, provide a description of any judicial or administrative proceedings involving the respondent material to respondent's business or financial capability, or to the subject matter of this solicitation, or that could interfere with respondent's performance of the work requested by this solicitation, including, but not limited to, any civil, criminal, or bankruptcy litigation; any debarment or suspension proceeding; any criminal conviction or indictment; and any order or agreement with or issued by a court or local, state, or federal agency.

Section 5. Nondiscrimination / Sexual Harassment Clause

Any contract entered into with a firm selected to provide services to PICA pursuant to this RFP (Contractor) shall contain, in substance, the following provisions:

1. In the hiring of any employee(s) for the manufacture of supplies, performance of work, or any other activity required under the contract or any subcontract, the Contractor, each subcontractor, or any person acting on behalf of the Contractor or subcontractor shall not discriminate by reason of race, gender, creed, color, sexual orientation, gender identity or expression, or in violation of the Pennsylvania Human Relations Act (PHRA) and applicable federal laws, against any citizen of this Commonwealth who is qualified and available to perform the work to which the employment relates.
2. Neither the Contractor nor any subcontractor nor any person on their behalf shall in any manner discriminate by reason of race, gender, creed, color, sexual orientation, gender identity or expression, or in violation of the PHRA and applicable federal laws, in the provision of services under the contract, or discriminate against or intimidate any employee involved in the

manufacture of supplies, the performance of work, or any other activity required under the contract.

3. Neither the Contractor nor any subcontractor nor any person on their behalf shall in any manner discriminate against employees by reason of participation in or decision to refrain from participating in labor activities protected under the Public Employee Relations Act, Pennsylvania Labor Relations Act, or National Labor Relations Act, as applicable and to the extent determined by entities charged with such acts' enforcement, and shall comply with any provision of law establishing organizations as employees' exclusive representatives.
4. The Contractor and each subcontractor shall establish and maintain a written nondiscrimination and sexual harassment policy and shall inform their employees in writing of the policy. The policy must contain a provision that sexual harassment will not be tolerated and employees who practice it will be disciplined.
5. The Contractor and each subcontractor shall not discriminate by reason of race, gender, creed, color, sexual orientation, gender identity or expression, or in violation of PHRA and applicable federal laws, against any subcontractor or supplier who is qualified to perform the work to which the contract relates.
6. The Contractor and each subcontractor represents that it is presently in compliance with and will maintain compliance with all applicable federal, state, and local laws, regulations and policies relating to nondiscrimination and sexual harassment. The Contractor and each subcontractor further represents that it has, where applicable, filed a Standard Form 100 Employer Information Report ("EEO-1") with the U.S. Equal Employment Opportunity Commission ("EEOC") and shall file an annual EEO-1 report with the EEOC as required for employers subject to Title VII of the Civil Rights Act of 1964, as amended. The Contractor and each subcontractor shall, upon request and within the time periods requested by the Commonwealth, furnish all necessary employment documents and records, including EEO-1 reports, and permit access to their books, records, and accounts by the contracting agency and the Bureau of Diversity, Inclusion and Small Business Opportunities for purpose of ascertaining compliance with provisions of this Nondiscriminatory/Sexual Harassment Clause.
7. The Contractor shall include the provisions of this Nondiscrimination/Sexual Harassment Clause in every subcontract so that those provisions applicable to subcontractors will be binding upon each subcontractor.
8. The Contractor's and each subcontractor's obligations pursuant to these provisions are ongoing from and after the effective date of the contract through the termination date thereof. Accordingly, the Contractor and each subcontractor shall have an obligation to inform PICA if, at any time during the term of the contract, it becomes aware of any actions or occurrences that would result in violation of these provisions.
9. PICA may cancel or terminate the contract and all money due or to become due under the contract may be forfeited for a violation of the terms and

conditions of this Nondiscrimination/Sexual Harassment Clause. In addition, PICA may proceed with debarment or suspension and may place the Contractor in the Contractor Responsibility File in the Commonwealth's Contractor Responsibility Program.