



ADDENDUM #1
REQUEST FOR PROPOSAL (RFP)
NO. 2026-024

Effective: March 24, 2026

Solicitation Title: IT Policy Assessment and Development

Issued by: City of Gaithersburg
Procurement Division
31 S. Summit Avenue
Gaithersburg, MD 20877

The purpose of this Addendum is to publish the questions received regarding this solicitation and the associated responses. This Addendum is incorporated into and made part of the above-named Request for Proposal (“Solicitation”). Except as amended herein, the terms and conditions of the Solicitation shall remain in full force and effect. The City is not responsible for the content of the questions and has provided the most comprehensive answers based on the interpretation of the questions.

The Solicitation is amended as follows:

1. Section 4.1, F, Pricing is replaced in its entirety with:

Pricing

This Section of the Proposal shall include a completed Price Proposal Sheet, duly signed by authorized person, based on the phases of the preliminary work plan as shown on the **Attachment B**, attached hereto. Additionally, fees for a la carte services and reimbursable expenses shall be delineated. The City will not reimburse for the following items: overtime, travel time, vehicle rental, fuel expenses, meals, lodging, per-diem.

2. ***New! Attachment B, Proposal Price Sheet, is added to this solicitation and attached to the end of this addendum.***

Below are the questions received and the City’s response:

1. Minimum Qualification: “50 Customers” Requirement

- Q1.1** How does the City define “50 customers” (e.g., distinct organizations, business units, program offices)?

A. “50 Customers” is defined by 50 unique business entities that paid for services similar to what is defined in the Scope of Work section of the RFP. These customers can be from any sector (e.g. Public, Private, Education) and can be combined by an Offeror’s representative (e.g. previous work, prior employment) to meet the requirement. However preference is for work performed for municipalities or government agencies of similar size and complexity as the City of Gaithersburg.

Q1.2 What specific evidence is required to verify the 50-customer requirement (client names, POCs, dates, etc.)?

A. A list of organizations that have paid the Offeror for services similar to what is defined in the Scope of Work section of the RFP.

Q1.3 Can the 50-customer requirement be satisfied through:

- a) experience of subcontractors? **Yes,**
- b) aggregated experience of prime + subcontractors? **Yes.**
- c) key personnel experience (including work performed prior to current firm)? **Yes.**
- d) Proposed subcontractor team/teaming partner provided in the table for performance? **Yes.**
- e) **Preference is for at least seven (7) years experience performing IT policy work outlined in this solicitation for government agencies or municipalities of similar size and complexity as the City of Gaithersburg.**

Q1.4 Is the 50-customer threshold a strict eligibility requirement or a benchmark/desired experience level?

A. No. Offerors can substitute years of experience from other customers to satisfy the requirement.

Q1.5 Would comparable experience in large or complex organizations be accepted in lieu of 50 distinct customers?

A. Yes, please see answers for Q1.1 and Q1.3.

Q1.6 Would the City consider revising the threshold to ensure broader competition consistent with small business participation objectives?

A. Yes. To be inclusive, Offerors can substitute staff with years of IT policy development experience from other businesses.

Q1.7 Does “50 customers” refer to customers, documents, or something else?

A. Refer to answer in Q1.1.

2. NIST Cybersecurity Framework (CSF) Version

Q2.1 Will the City accept or prefer alignment with NIST CSF 2.0, given it is the current standard?

A. Yes

Q2.2 Should proposals include a NIST CSF 1.0 mapping or crosswalk?

A. Yes

Q2.3 If CSF 2.0 is allowed, should deliverables still demonstrate CSF 1.0 compliance?

A. No

3. Work Modality (On-Site vs Remote)

Q3.1 Are there expectations for on-site work, and if so, what percentage of assessment activities must be on-site?

A. There is no expectation that the work performed for the City will be done onsite. However, the tabletop exercise shall be performed on-site.

Q3.2 Will vendor work be remote, onsite, or hybrid?

A. Hybrid. Most of the documentation can be performed remotely. However, that tabletop exercise will need be performed on-site.

Q3.3 Should the tabletop exercise be delivered on-site or remotely?

A. On-site.

Q3.4 Is a virtual tabletop exercise acceptable?

A. No.

4. Budget / Contract Funding

Q4.1 What is the maximum expected value or budget allocated for this contract?

A. The City does not wish to disclose the amount of funding allocated for this RFP.

Q4.2 Does the City have cost limitations or an anticipated budget target?

A. Yes.

Q4.3 Can the City confirm whether the project is grant-funded at \$98,000 per the published budget?

A. The project is funded via a grant.

5. Existing Policies: Inventory, Maturity, and Scope

Q5.1 How many existing IT policies does the City currently have?

A. The City has both an Administrative policy which is located on our website (www.gaithersburgmd.gov) and internal policies that will be furnished to the successful Offeror once the contract has been awarded.

Q5.2 Which policies need to be updated vs. created from scratch?

A. This will be discovered at kickoff.

Q5.3 Will the City provide all existing IT policies, IRPs, vulnerability procedures, and COOP/EOP materials at kickoff?

A. Yes.

Q5.4 The scope lists ten policy areas in Section 2.4.A.iii but does not specify expected depth or length for each.

- a) Are Offerors expected to perform a gap analysis, develop new documents, or both? **Both**
- b) What level of detail is expected for each policy document? **The level of detail that is consistent with a complete set of policies.**
- c) Which of these City of Gaithersburg policy documents exist now or will need to be developed out of the following policies referenced? **This question will be answered at kickoff.**

Q5.5 Can the City provide an approximate number of existing internal IT policies that will need to be assessed and updated, as opposed to policies that must be created entirely from scratch?

A. This question will be answered at kickoff time to the successful Offeror.

Q5.6 The number and types of critical applications are not specified. How many critical applications does the City operate, and what are the primary platforms?

A. This question will be answered at kickoff time to the successful Offeror.

6. Training Requirements

Q6.1 What format does the City prefer for policy awareness and staff training (virtual, on-site, email campaign)?

A. On-Site

Q6.2 Should the Contractor deliver live sessions, recorded modules, or train-the-trainer?

A. Tabletop will be on-site live sessions.

Q6.3 For recurring training, should materials and a training plan be included as deliverables?

A. A training plan should be included with proposal submission.

Q6.4 Should training be SCORM-compliant for use in the City's LMS?

A. No.

7. COOP/EOP Integration

Q7.1 Will the City provide current COOP/EOP documentation?

A. Yes.

Q7.2 What level of integration is expected between IRP procedures and COOP/EOP?

A. This expertise is expected from the Consultant.

7.3 What is the current status and maturity of COOP/EOP plans?

A. The COOP/EOP plans were last revised in 2009.

8. Legal & HR Review Cycles

Q8.1 Section 2.3, A notes that deliverables must be reviewed by Legal and adopted by HR. Should the Contractor provide documentation to support legal/HR review, or will the City manage approvals?

A. The City will manage approvals.

Q8.2 How many rounds of review (legal + HR) should the Offeror expect?

A. A minimum of one, however it should be based on the Consultant's expertise.

Q8.3 How many revisions should Offerors include in the schedule?

A. This should be based on the Consultant's expertise.

9. Staff Participation & Responsibilities

Q9.1 Does the City anticipate constraints on staff availability for interviews, workshops, and tabletop exercises?

A. No.

Q9.2 Who will serve as the primary City liaison, and what is their expected availability?

A. Guy Goodenough will be the primary liaison and will be available throughout the duration of the project.

Q9.3 What internal responsibilities will the City handle (scheduling, communications, SME coordination)?

A. The City will guide the effort to coordinate meetings scheduled with City staff.

Q9.4 RTO/RPO Availability: The RFP mentions the City will provide RTO/RPOs. If these are not currently defined, does the City expect the Contractor to facilitate the Business Impact Analysis (BIA) required to generate them?

A. Yes. The City anticipates the Offeror will gather/create any documentation needed to address RTO/RPO.

10. Cloud Environment & Technical Scope

Q10.1 What cloud platforms and services are currently in use?

A. The City uses several cloud platforms. This information will be presented to the Offeror at kickoff.

Q10.2 What is the approximate split between on-premise and cloud environments?

A. 60/40

Q10.3 Does the City maintain an existing asset inventory?

A. Yes.

Q10.4 Are IT assets already classified/categorized?

A. No. However, this deficiency is being handled currently by another initiative.

Q10.5 Is there a Vulnerability Management Program in place?

A. Yes. The Vulnerability Management Program has been in place informally for 12 years and formally for approximately 5 years.

11. AI Policies

Q11.1 Does the City have existing AI usage guidelines? What current AI tools or services are currently in use or under consideration?

A. Yes

Q11.2 Should the AI policy:

- a) Be a general staff use policy, or
- b) Be a technical/security framework for AI-enabled applications?
- c) Address topics such as employee use of AI tools, vendor use of AI technologies, data protection and sensitive information handling, and procurement or approval processes for AI tools?

A. The AI policy should address all of the above.

12. Tabletop Exercise

Q12.1 Which departments/teams will participate in the tabletop exercise?

A. This will be determined during the engagement.

Q12.2 How many participants are expected?

A. This will be determined during the engagement.

Q12.3 How many tabletop exercises must the vendor deliver?

A. We are looking for the Offeror to make a recommendation.

Q12.4 Should the vendor provide the venue, catering, or other logistics?

A. No.

Q12.5 Should the testing plan include schedules, roles, evaluation criteria, and after-action templates?

A. Yes. The City anticipates conducting biannual tabletop exercises as outlined by the Offeror.

13. Critical Applications & Environment

Q13.1 How many critical applications does the City operate, and what platforms do they run on?

A. This will be answered in the kickoff meeting or during the initial engagement process.

Q13.2 Has the City performed a prior NIST CSF assessment?

A. Yes.

14. Additional Deliverable Clarifications

Q14.1 Should procedures (referenced in 2.3) be included even though they aren't explicitly listed in 2.4 deliverables? Section 2.3,C,iv, requires developing procedures that complement IT policies, but Section 2.4,A, does not list procedures as deliverables. Should IT policy procedures be included as formal deliverables?

A. Yes. The IT policy procedure should be included as a formal deliverable.

Q14.2 Should vulnerability classification schemas, reporting workflows, and prioritization methods be delivered as standalone documents or incorporated into policy documents listed in section 2.4?

A. The City will leave this process to the expertise of the Offeror.

Q14.3 Should cyber forensics guidance or procedures be included as a deliverable?

A. No.

Q14.4 Should external incident-reporting mechanisms include design recommendations or formal documentation?

A. It should include design recommendations but not formal documentation.

Q14.5 Section 2.3,F, vi, requires identifying current control measures and recommending mitigations. Should a control-gap analysis report be included?

A. Yes. A gap analysis should be included.

Q14.6 Should risk tolerance matrices align with an existing City framework or be proposed by the vendor?

A. Current Risk tolerance matrices should be evaluated and a recommendation issued.

Q14.7 What level of detail is expected in each policy document?

A. We are relying on the Consultant's expertise.

Q.14.8 How is vulnerability data communicated and reported to stakeholders?

A. Communication is predicated on severity and impact to stakeholder(s).

15. Contract Timing

Q15.1 What is the anticipated start date?

A. The anticipated start date is estimated upon Offeror receiving a Notice of Intent to Award notification and completion of an executed agreement with the City.

Q15.2 Must all work be completed by 12/31/2026?

A. Yes, unless circumstances dictate otherwise, all work must be completed by the date specified in the RFP.

16. Miscellaneous

Q16.1 I am asking for clarification on what registration is required and where to obtain it; citing “Be registered and in good standing to provide services in the state of Maryland”?

A. Offerors need to contact SDAT in Maryland for a Certificate of Good Standing or other filing verifying the Offeror is in Good Standing with the *Department of Assessments and Taxation of Maryland*. Certificates of Status may be obtained online at <https://egov.maryland.gov/BusinessExpress/>. This requirement applies to both domestic and foreign Offerors (out of state). Foreign entities should contact the State Department of Assessments and Taxation, 301 West Preston Street, Baltimore, Maryland 21201, to determine and apply for the appropriate documentation.

Q16.2 Need to know if responding companies can prime the contract and use registered sub-contractors to deliver services?

A. Section 4 of the solicitation outlines that prime contractor may list subcontractors on the required forms in Attachment A.

Q.16.3 Is there an incumbent currently delivering these services, or is this a new engagement?

A. This is a new engagement.

Q.16.4 Have similar assessments been conducted previously? If so, when was the last engagement?

A. No.

Q.16.5 Does the City have preferred templates, branding, or formatting standards for policy and procedure documents?

A. This will be discovered at kickoff or during the initial engagement process.

Q.16.6 When the City mentions RPO and RTO are they referring to traditional data protection/recovery/Backup/DR techniques to satisfy these?

A. Yes.

Q.16.7 What back-up software and hardware is the City using today?

A. This will be discovered at kickoff or during the initial engagement process.

Q.16.8 Is proprietary software acceptable in your environment?

A. Yes.

Q.16.9 Section 8.2 indicates that payment milestones will be established after contract award. Can the City share the anticipated milestone framework it envisions so that Offerors may structure pricing and project phasing accordingly?

A. Please complete the new Attachment B, Proposal Price Sheet.

Q.16.10 Does the City currently maintain an enterprise risk management methodology or risk scoring framework that the risk tolerance matrix should align with?

A. No.

Q.16.11 Should the Incident Response Plan include specific incident playbooks (e.g., ransomware response, data breach response), or should the deliverable focus on a framework-level incident response process aligned to NIST CSF?

A. The deliverable should focus on a framework-level incident response process aligned to NIST CSF.

Q.16.12 Is the contractor expected to produce a formal After-Action Report (AAR) summarizing lessons learned and recommended improvements following the tabletop exercise?

A. Yes.

Q.16.13 The RFP requests development of policy documentation as well as a tabletop exercise to test the Incident Response Plan. Should offerors prioritize delivering

comprehensive policy documentation, or does the City place equal emphasis on operational readiness and staff preparedness when evaluating proposals?

A. While the intent of the RFP is to further mature and create missing policy, the City views the tabletop exercise as an important part of the engagement.

Q16.14 Does the City have a preferred format or template for the cost proposal, or may offerors structure the pricing breakdown at their discretion provided it clearly identifies all costs?

A. Please complete the new Attachment B, Price Proposal Sheet.

Q16.15 Are all IT systems protected using the same security controls, or are there designated critical or special-purpose systems that follow different security standards or controls?

A. This will be discovered at kickoff or during the initial engagement process.

Q16.16 Are IT systems configured according to CIS Benchmark best practices, and are configuration changes monitored and tracked?

A. This will be discovered at kickoff or during the initial engagement process.

Q16.17 If selected, is the City able to share Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for critical systems?

A. Yes.

Q16.18 How are cybersecurity metrics currently captured and reported? Which systems or platforms are used to track these metrics?

A. This will be discovered at kickoff or during the initial engagement process.

Q16.19 How are vulnerabilities prioritized for remediation? Is there an emergency or expedited patching process in place for critical vulnerabilities?

A. This will be discovered at kickoff or during the initial engagement process.

- Q16.20** Do you currently use any vulnerability scanning tools or patch management systems?
- A. Yes.**
- Q16.21** What cyber and infrastructure risks are leadership most concerned about right now?
- A. This will be discovered at kickoff or during the initial engagement process.**
- Q16.22** How does the City define the success of this project?
- A. The City will deem this a successful project if the City receives the defined policy set and tabletop exercise defined by the RFP.**
- Q16.23** Contract Period and Renewals (2.7.B) - By mutual agreement of parties, the resultant contract will be automatically renewed at existing prices, terms and conditions. Will there be an optional number of years for continuance of documentation needed for this contract?
- A. No. At this time we expect the project to be completed 12/31/2026. If project extends beyond that time, then contract will be amended at existing prices and rates.**
- Q16.24** Will the Prime Contractor be responsible for providing security background checks for its personnel as well as its subcontractors, or the City take on that responsibility?
- A. We do not perform security background checks however every Offeror attest to the truthfulness of disclosure of any debarment from federal, state programs, liens and litigations on your firm and any criminal convictions for fraud and embezzlement. Failure to disclose can lead to cancellation of awarded contracts and future debarment from federal, state, and city contracts.**
- Q16.25** **Payments (8.2)** - states that the Contractor will be paid following the completion of milestones – to be later established and agreed upon. Will this happen before the contract becomes final and signed off by all?
- A. Yes, the new Attachment B, Price Proposal Sheet will be incorporated into executed contract between vendor and the City.**
- Q16.26** **Invoices, Payment Terms and Taxes (7.36)** - States the City will only pay proper invoices with a net 30-day payment; but wants consideration for discount if pay earlier. Should early payment (Prompt Payment) discounts be added in the pricing structure.

A. No, prompt pay discounts should not be factored into the pricing proposal structure.

Q16.26 Should pricing include multi-years? Should pricing be based on a specific number of documents created? If so, what is the number?

A. Project concludes at the end of 2026 therefore a multi-year deal is unnecessary. Pricing should be based by phases as outlined in the Attachment B, Proposal Price Sheet, and not the amount of documents created.

Q16.27 Proposed Staff (4.1.C.i) - States to include resumes for all Staff Proposed along with their qualifications and experience performing the work. Are you looking for personnel to be certified or will years of experience be acceptable?

A. Either is acceptable. However, the City views a combination of certification and experience as the strongest candidate.

~End of Addendum~



City of Gaithersburg

Proposal Price Sheet

Attachment B

Solicitation No. RFP2026-024

The Offeror shall complete this form in its entirety and return it with their Proposal. The Offeror is expected to review the Solicitation Document in its entirety and to understand project requirements and work scope prior to submitting a Proposal.

City of Gaithersburg Policy Assessment and Development

<i>Section I: Work Plan Phases</i>		
Line #	Project Initiation and Planning	Total Price
01	Initial Consultation/Kick-off Meeting	\$
02	City Document/Policy Review	\$
	Data Collection and Review	Total Price
03	Data Analysis	\$
04	Draft of Documentation/HR/Legal Review	\$
	Documentation and Presentation	Total Price
05	All Document Deliverables- IT Policy, IRP, Vulnerable Management Policy	\$
06	Tabletop Exercise Training	\$
	Other (Specify)	\$
	<i>Subtotal Section I:</i>	\$
	<i>Profit and Overhead</i>	\$
	<i>Total Section I:</i>	\$

<i>Section II: Miscellaneous Expenses (if applicable)</i>			
Item #	Description	Unit Cost (\$) x Units	Total Cost (\$)
1		\$	\$
2		\$	\$
3		\$	\$
4		\$	\$
5		\$	\$
6		\$	\$

Note: Fees for a la carte services and reimbursable expenses shall be delineated. The City will not reimburse for the following items: overtime, travel time, vehicle rental, fuel expenses, meals, lodging, per-diem unless approved by the City for Consultant to meet work scope.

By my signature, I hereby testify that I am a duly authorized representative of the firm and that I have fully entered, examined, and reviewed the items and totals represented on this Proposal Price Sheet and they are accurate and complete.

Company Name: _____

Signature: _____

Date: _____

Print Name: _____

Title: _____