

ATLANTA REGIONAL COMMISSION

Enterprise Backup, Recovery & Disaster Recovery Solution

REQUEST FOR PROPOSAL

July 15, 2026

Proposals Due: August 14, 2026 by 5:00 p.m. EST

Purpose and Background

The Atlanta Regional Commission (ARC) is a regional planning and intergovernmental coordination agency serving the 11-county Atlanta metropolitan area and its municipalities. The ARC Office of Information Technology relies on a broad portfolio of on-premises, cloud, and SaaS-hosted systems to support the agency's work program across the areas of community development, transportation planning, workforce development, aging services, natural resources, research, urban area security, and general administrative functions.

ARC is issuing this Request for Proposal (RFP) to solicit competitive offers for the design, supply, implementation, and ongoing support of an enterprise-class Backup, Recovery, and Disaster Recovery (BR/DR) solution. The solution must provide comprehensive data protection across ARC's hybrid environment, establish immutable backup storage, replicate protected data to an off-site cloud platform, and deliver recovery capabilities capable of meeting Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) measured in minutes.

Note: ARC is not seeking a Backup as a Service (BaaS) or Disaster Recovery as a Service (DRaaS) team to assume ongoing backup recovery or disaster recovery operations.

Proposal Submittal

All proposals must be submitted electronically through the Atlanta Regional Commission (ARC) procurement website. Proposal submitted by any other method (including email, mail, fax, or hand delivery) may not be accepted unless specified in the solicitation document.

Respondents must register and complete the application on the ARC procurement website to submit a proposal. It is the responsibility of the respondent to ensure successful registration and timely submission.

Proposals must be received no later than **Friday, August 14, 2026, by 5:00 p.m. EST**. The procurement system will automatically record the date and submission. Late proposals will not be accepted under any circumstances.

The Respondent(s) is solely responsible for:

- Uploading all required documents;
- Verifying that files are complete, readable, and properly labeled; and
- Ensuring submission is finalized prior to the deadline.
- Only one proposal containing all required information may be uploaded per responder (the system will only submit the latest uploaded).

ARC is not responsible for technical difficulties, internet outages, user errors, or system delays experienced by the respondent. Respondents are strongly encouraged to submit proposals well in advance of the deadline.

Upon successful submission, the system will provide email confirmation. This confirmation serves as proof of receipt.

Vendors with questions regarding this RFP must submit them through ARC procurement portal at <https://procurement.atlantaregional.org/opportunities/>. Questions submitted after the deadline or through any other means will not be considered. All questions and official responses will be published to the ARC website per the schedule in the timeline below. Only written responses issued through the website shall be considered official and binding.

To ensure fairness and transparency, respondents are prohibited from contacting ARC staff, board members, or consultants regarding this solicitation outside of the formal Q&A process.

It is the responsibility of each respondent to regularly check the procurement website for addenda, clarifications, and updates. Failure to review posted addenda shall not relieve a respondent from compliance with any requirements of the RFP.

Milestone	Date / Deadline
RFP Release Date	Wednesday, July 15, 2026
Deadline for Questions	Friday, July 24, 2026, by 5:00 p.m. EST
ARC Responses to Questions Posted	Friday, July 31, 2026
Proposals Due	Friday, August 14, 2026, by 5:00 p.m. EST

Proposals shall not exceed 20 pages (8.5 x 11 inches), printed double sided, inclusive of credentials and experience. Cover pages, end sheets, budget exhibits, introductory letters, and product details are excluded from the page count. Minimum font size is 12 points throughout.

If interviews are deemed necessary, a short list of service providers will be invited to participate in an evaluation committee interview. ARC will confirm date and time of any interviews with selected firms. ARC reserves the right to award this contract based on initial proposals without formal interviews, and to award all or part of this project to one or more firms.

ARC further reserves the right to: select a proposal other than the lowest-cost submission; reject any or all proposals or portions thereof; waive or modify irregularities or inconsistencies in proposals; request modifications to proposals from any respondents during contract review and negotiation; and negotiate any aspect of proposals with one or more proposers simultaneously.

Restriction of Communication

From the date of the advertisement of the solicitation through contract award and selection is announced, respondents are not allowed to communicate about this solicitation or scope with any staff of ARC, except for submission of questions as instructed in the RFP or as provided by any existing work agreement(s). In the case of violation of this provision, ARC reserves the right to reject the submittal of the offending respondent.

Minimum Qualifications

To be considered for award, proposing vendors must demonstrate the following minimum qualifications:

- The vendor's primary backup and data protection platform must be a commercially available, production-released product with an established install base in the state and local government or public sector market.
- The vendor or its authorized implementation partner must have successfully deployed a similar enterprise BR/DR solution for at least three (3) government or regulated-industry clients within the past five (5) years, with references available upon request.
- The vendor must maintain SOC 2 Type II certification (or equivalent) for any cloud-hosted components included in the proposal.
- The vendor must maintain FedRAMP authorization or StateRAMP equivalency for any cloud services proposed as the off-site replication target or clearly document the path to compliance.

Proposal Response Requirements

Vendors shall organize their proposal to address each of the following sections:

- Legal name of the firm.
- Point of contact (name, title, phone number, mailing address, and email address) at the lead firm.
- Executive Summary — high-level overview of the proposed solution and vendor qualifications.
- Technical Approach — detailed description of the proposed architecture, components, and methodology for meeting all listed requirements.
- RTO/RPO Capability Statement — specific documentation of how the proposed solution achieves RTOs and RPOs within minutes for Tier 1 workloads, including references to tested performance benchmarks.
- Immutability and Security Architecture — description of immutable storage implementation, ransomware protection mechanisms, and alignment to NIST 800-53 and HIPAA requirements.
- Cloud Replication Architecture — proposed cloud target platform, replication topology, encryption approach, and immutability controls in the cloud tier.
- Implementation Plan — proposed project timeline, milestones, and staffing plan.
- Listing of key personnel and qualifications.
- References — minimum three (3) client references for comparable deployments.
- Pricing — itemized pricing for all hardware, software licenses, professional services, and annual maintenance, presented in a format that allows ARC to evaluate total cost of ownership over a five (5) year period.
- Exceptions — any proposed exceptions to this Scope of Work must be clearly identified and justified.

The successful service provider should be prepared to begin work immediately upon contract execution. ARC reserves the right to award all or part of the available funds for this project.

Contract Terms

The initial contract term shall be three (3) years, with two (2) optional one-year renewal periods at ARC's discretion, for a maximum potential term of five (5) years. The contract structure shall be hardware and software purchase with annual maintenance and support. Pricing for renewal periods must be included in the initial proposal.

ARC reserves the right to negotiate contract terms, request best-and-final offers, award to multiple vendors, or cancel this procurement at any time without obligation. This Scope of Work is issued for planning and competitive solicitation purposes and does not constitute a commitment to award a contract.

Conflict of Interest and Confidentiality

ARC is subject to the Georgia Open Records Act. All submitted proposals become public records upon request. Any information containing trade secrets or proprietary data, as defined under Georgia state law, must be clearly marked as "Confidential" on the specific pages or sections containing such information. Marking an entire proposal as confidential will not be honored.

Respondents must disclose any potential conflicts of interest that may arise from the provision of services described in this RFP. Required disclosures must include: (1) the name of the individual(s) with whom a conflict exists; (2) all relevant facts pertaining to the potential conflict; and (3) a description of internal controls proposed to mitigate the conflict. ARC's Staff Legal Counsel will determine whether any disclosed conflict presents an organizational conflict of interest that would preclude award.

Conflicts of interests are governed by the ARC Standards of Ethical Conduct, available on the ARC website.

Evaluation Criteria

Proposals will be evaluated on a best-value basis using the following weighted criteria:

Category	Requirement	Weight
Technical Capability	Degree to which the proposed solution meets or exceeds the functional, performance, security, and compliance requirements defined in this Scope of Work.	35%
RTO/RPO Performance	Demonstrated ability to achieve sub-5-minute RTOs and RPOs; quality of supporting evidence.	20%
Implementation Approach	Quality and realism of the proposed implementation plan, timeline, and staffing.	20%
Vendor Qualifications	Relevant experience, client references, certifications, and financial stability.	10%
Total Cost of Ownership	5-year TCO including hardware, software, professional services, and maintenance.	5%
Support and SLAs	Quality and responsiveness of proposed support model; clarity of SLA commitments.	10%

Exhibit A: Scope of Work

In-Scope Workloads and Systems

The awarded vendor shall provide data protection coverage for all of the following ARC workload categories:

- Virtualized infrastructure — virtual machines hosted on on-premises hypervisor platforms (VMware vSphere and/or Microsoft Hyper-V), ranging from 50 to 70 VMs across approximately 50–200 TB of usable data.
- Physical servers — bare-metal servers running Windows Server and/or Linux operating systems.
- Cloud workloads — IaaS and PaaS resources hosted in one or more public cloud environments (e.g., Microsoft Azure, Amazon Web Services, Google Cloud Platform), as mutually defined during the discovery and design phase.
- Microsoft 365 and SaaS applications — protection of Exchange Online, SharePoint Online, OneDrive for Business, and Teams data at minimum; additional SaaS application coverage to be identified during the design phase.
- Structured databases — Microsoft SQL Server, PostgreSQL, and other enterprise databases as identified during discovery; protection must be application-consistent and support granular object-level recovery.

Core Functional Requirements

The solution shall fulfill the following core capabilities:

Backup and Snapshot Management

Policy-based backup scheduling with configurable retention tiers (daily, weekly, monthly, yearly).

- Application-consistent snapshot support for all in-scope hypervisor and database workloads.
- Incremental-forever or similar change-block-based technology to minimize backup windows and storage consumption.
- Automated catalog and indexing of all protected assets to support fast search and granular recovery.

Immutable Storage

- All backup data stored on-premises shall reside on WORM-compliant (Write Once, Read Many) or object-locked immutable storage.
- Immutability policies shall be enforced at the storage platform level and shall not be defeatable by operating system or application-layer credentials, including backup administrator accounts.
- The solution shall support a dual-administrator or multi-party authorization model to prevent unauthorized deletion or modification of protected data.
- Immutability configurations shall align with NIST SP 800-53 control families including AU (Audit and Accountability), SI (System and Information Integrity), and CP (Contingency Planning).

Cloud Replication and Off-Site Copy

- The solution shall replicate backup data to a vendor-proposed or ARC-designated cloud platform, creating a geographically separated secondary copy of all protected workloads.
- Cloud replication shall occur on a configurable schedule with a minimum replication frequency of 15 minutes for Tier 1 (critical) systems.
- Data in transit to and from cloud replication targets shall be encrypted using TLS 1.2 or higher.
- Data at rest in cloud storage shall be encrypted using AES-256 or equivalent.
- The vendor's proposed cloud target architecture shall support object-lock or equivalent immutability controls, providing air-gap-equivalent protection against ransomware and malicious deletion.
- The solution shall provide clear visibility into replication status, lag time, and cloud storage consumption through a unified management console.

Recovery Capabilities and Target SLAs

- The solution shall support RTOs and RPOs as low as a few minutes for designated Tier 1 critical workloads.
- Recovery methods shall include, at minimum: full restore, granular file/object restore, instant VM recovery (live mount), and database log replay for point-in-time recovery.
- Instant recovery or live mount capabilities shall allow a VM to boot and serve production traffic directly from the backup repository while a full restore completes in the background.
- The solution shall support cross-hypervisor and cross-platform recovery (e.g., recover a VMware VM to Hyper-V, or to a cloud IaaS instance) to support failover scenarios.
- Disaster recovery orchestration shall include automated runbooks or DR workflow automation enabling multi-system failover with minimal manual intervention.
- Automated DR testing shall be supported on a non-disruptive, sandboxed basis without impacting production or backup operations.

Architecture and Integration Requirements

- The solution shall integrate natively with ARC's existing hypervisor, operating system, and database platforms without requiring agent-based deployment on every protected virtual machine (agentless architecture preferred for virtual workloads).
- The solution shall provide a single-pane-of-glass management interface capable of managing on-premises backup, cloud replication, and DR orchestration.
- RESTful API access shall be provided to support integration with ARC's existing ITSM and monitoring toolsets.
- Role-based access control (RBAC) shall be supported with granular permissions aligned to ARC's organizational structure.
- Multi-factor authentication (MFA) shall be supported for all administrative access to the management platform.
- The solution shall integrate with ARC's Active Directory / Entra ID environment for identity and access management.
- SIEM integration (syslog, API, or native connector) shall be supported for forwarding security-relevant events and alerts.

Compliance and Security Requirements

The solution and all associated vendor services shall support ARC's compliance obligations under the following frameworks:

- NIST Special Publication 800-53 (Rev. 5) — The solution architecture and operational procedures shall map to applicable controls, with particular emphasis on CP-9 (Information System Backup), CP-10 (Information System Recovery and Reconstitution), SI-12 (Information Handling and Retention), and SC-28 (Protection of Information at Rest).
- HIPAA Security Rule — The solution shall support the technical safeguard requirements of 45 CFR Part 164, Subpart C, including audit controls, integrity controls, and transmission security, for systems that store or process Protected Health Information (PHI) associated with ARC's Area Agency on Aging programs.
- The vendor shall provide documentation demonstrating how the proposed solution maps to NIST 800-53 and HIPAA technical safeguard requirements.
- The vendor shall disclose any active data breach incidents, consent orders, or regulatory actions affecting their platform or cloud services within the past three years.

Professional Services — Implementation

The vendor's proposal shall include a comprehensive professional services engagement covering:

- Discovery and Assessment — Vendor shall conduct a structured discovery of ARC's existing environment, document all in-scope workloads, and validate sizing assumptions prior to finalizing the solution design.
- Solution Design — Vendor shall produce a detailed architecture document including topology diagrams, data flow documentation, sizing calculations, and a mapping of the proposed solution to ARC's RTO/RPO requirements by workload tier, including any preferred or required emergency hosting services or sites to facilitate DR operations.
- Deployment and Configuration — Vendor shall be responsible for full installation, configuration, and commissioning of all hardware, software, and cloud components included in the proposal.
- Policy and Runbook Development — Vendor shall work with ARC staff to define backup policies, retention schedules, and DR runbooks for all workload tiers.
- Testing and Validation — Vendor shall conduct a formal acceptance test including at least one full DR simulation test prior to transitioning to production support.
- Knowledge Transfer and Training — Vendor shall provide hands-on administrator training for ARC IT staff covering day-to-day operations, policy management, recovery procedures, and DR test execution.

Ongoing Support and Maintenance

The contract shall include hardware and software maintenance and support, covering:

- Hardware maintenance providing next-business-day (NBD) on-site parts and labor for all vendor-supplied appliances, with an option to upgrade to 4-hour response for Tier 1 components.
- Software support providing access to all product updates, patches, and major version upgrades throughout the contract term.
- Technical support access available 24 hours per day, 7 days per week, 365 days per year for Severity 1 (production-down or imminent data-loss) incidents.
- A designated technical account manager or customer success resource for quarterly business reviews and proactive health monitoring.
- Proactive alerting and monitoring integration providing automated notifications of backup failures, replication lag breaches, storage capacity thresholds, and security-relevant events.

Deliverables Summary

Category	Requirement
Discovery & Design	Completed environment discovery report; detailed solution architecture document with topology diagrams and RTO/RPO workload mapping.
Implementation	Fully installed, configured, and tested BR/DR environment including on-premises hardware/software and cloud replication components.
Policies & Runbooks	Documented backup policies, retention schedules, and DR runbooks for all workload tiers.
Acceptance Testing	Formal acceptance test report including DR simulation results signed off by ARC IT leadership.
Training	Administrator training delivered to ARC IT staff; training materials provided in electronic format.
Documentation	As-built architecture documentation; NIST 800-53 and HIPAA control mapping documentation.
Ongoing Support	24x7x365 support, software maintenance, and quarterly business reviews throughout the contract term.

Exhibit B: Compensation

Method of Payment

The awarded vendor shall submit invoices documenting work performed during the invoice period. ARC will pay or reject properly submitted invoices within 45 days of receipt. ARC may, at its reasonable discretion, disallow any work not properly documented in the required progress report.

Final Payment: Final payment will be made only upon ARC's determination that all contractual requirements have been fulfilled. The awarded vendors final invoice and final narrative progress report must be received by ARC no later than fifteen (15) days after the project completion date specified in the contract. ARC may disallow all or part of a final invoice after this deadline.

Invoice Submission: Invoices must be submitted and directed to:

IT Purchasing | 229 Peachtree St NE, Suite 100, Atlanta, Georgia 30303 |
itpurchasing@atlantaregional.org

Each invoice must include a description of the work completed; percentage of work completed; amount previously billed; a unique invoice number; the performance period; and a valid payment address. Subcontractor payments must be itemized on invoices, including notation on DBE/MBE/WBE status where applicable.

Exhibit B-1 — Proposed Cost Breakdown

Service Area	Proposed Amount
Hardware Requirements	\$
Licensing and Support	\$
Cloud Services / Immutable Storage	\$
Onboarding and Training	\$
Implementation	\$
TOTAL	\$

Appendix A —Resource Sizing

The following table summarizes ARC's environment. This information is provided to assist vendors in scoping their proposals.

Resource	Description / Device
Virtualized Servers	47 (windows, linux)
Bare Metal Servers	8 (windows), 6 virtual hosts
Block Storage Volume	27 TB
Server Data Types	Structured (10 TB) and Unstructured (45 TB)
Database	MS-SQL, PostgreSQL
SMB Storage	95 TB (cloud hosted)
ISP Connectivity	10 GbE bandwidth
Cloud / SaaS	AWS, Azure, Microsoft365 hybrid
Retention	90 days minimum, 6 months desired

Compliance Frameworks

- HIPAA
- ISO 27001
- NIST SP 800-53

Required Forms

The following forms must be completed, signed, and included with the submitted proposal:

- Georgia Security and Immigration Compliance Act Affidavit (Contractor Affidavit)
- Contractor/Vendor Information Form
- Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion – Lower Tier Covered Transactions and Lobbying

Blank copies of each form are attached to this RFP.

**GEORGIA SECURITY AND IMMIGRATION COMPLIANCE ACT AFFIDAVIT
CONTRACTOR AFFIDAVIT**

By executing this affidavit, the undersigned person or entity verifies its compliance with O.C.G.A. §13-10-91. stating affirmatively that the individual, firm or entity which is engaged in the physical performance of services under a contract with the Atlanta Regional Commission has registered with and is participating in a federal work authorization program, in accordance with the applicability provisions and deadlines established in O.C.G.A. 13-10-91.

The undersigned person or entity further agrees that it will continue to use the federal work authorization program throughout the contract period, and it will contract for the physical performance of services in satisfaction of such contract only with subcontractors who present an affidavit to the undersigned with the information required by O.C.G.A. 13-10-91(b).

The undersigned person or entity further agrees to maintain records of such compliance and provide a copy of each such verification to the Atlanta Regional Commission within five (5) business days after any subcontractor is retained to perform such service.

EEV / E-Verify™ Company Identification Number

Date of Authorization

Company Name

Signature of Authorized Officer or Agent

Title of Authorized Officer or Agent

Printed Name of Authorized Officer or Agent

SUBSCRIBED AND SWORN
BEFORE ME ON THIS THE

_____ DAY OF _____, 2026

Notary Public

[NOTARY SEAL]

My Commission Expires: _____

**CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY
AND VOLUNTARY EXCLUSION – LOWER TIER COVERED TRANSACTIONS AND LOBBYING**

1. DEBARMENT, SUSPENSION, INELIGIBILITY AND VOLUNTARY EXCLUSION- LOWER TIER COVERED TRANSACTIONS

The prospective lower tier participant agrees by submitting this proposal that, should the proposed covered transaction be entered into, it shall not knowingly enter into any lower tier covered transaction with a person who is proposed for debarment under 45 CFR Part 76, debarred, suspended, declared ineligible, or voluntarily excluded from participation in this covered transaction, unless authorized by the department or agency with which this transaction originated.

The terms "covered transaction", "debarred", "suspended", "ineligible", "lower-tier covered transaction", "participant", "person", "primary covered transaction", "principal", "proposal", and "voluntarily excluded", as used in this clause have the meaning set forth in the Definitions and Coverage sections of rules implementing Executive Order 12549.

The prospective lower tier participant certifies that, by submission of this proposal, that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any Federal department or agency.

Where the prospective lower tier participant is unable to certify to any of its statements in this certification, such prospective participant shall attach an explanation to this proposal.

2. LOBBYING

As required by Section 1352, Title 31 of the U.S. Code (as implemented at 45 CFR Part 93), the applicant certifies that to the best of his or her knowledge and belief that:

- (1) No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.
- (2) If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.
- (3) The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by Section 1352, Title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure.

Statement for Loan Guarantees and Loan Insurance

The undersigned states, to the best of his or her knowledge and belief, that:

If any funds have been paid or will be paid to any persons for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this commitment providing for the United States to insure or guarantee a loan, the undersigned shall complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.

Submission of this statement is a prerequisite for making or entering into this transaction imposed by Section 1352, Title 31, U.S. Code. Any person who fails to file the required statement shall be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure.

As the duly authorized representative of the applicant, I hereby certify that the applicant will comply with the above applicable certification(s).

NAME OF APPLICANT

AWARD NUMBER and/or PROJECT NAME

PRINTED NAME OF AUTHORIZED REPRESENTATIVE

TITLE OF AUTHORIZED REPRESENTATIVE

SIGNATURE OF AUTHORIZED REPRESENTATIVE

DATE

REV ARC 05/08

CONTRACTOR/VENDOR INFORMATION

**Legal name & address
of entity:**

If different from above-

Legal name of Payee:

Payment Address:

(If additional addresses are needed, identify each and its purpose on the reverse of this page.)

Legal entity status (please mark all that apply):

☐ Corporation/C-Corp LLC/S-Corp LLC	☐ Individual/Sole-Proprietor/Single Member LLC
☐ Partnership/LLC Partnership/LLP	☐ Government: Federal/State/Local/Authority
☐ Non-Profit: 501(c)(3)/501(c)(4)	☐ Other: (describe) _____

(Federal) Employer Identification Number: _____

OR

Social Security Number (for an individual): _____

Is this contractor/vendor an attorney/law firm? YES _____ NO _____

Is this contractor/vendor debarred, suspended, ineligible or excluded from participation in federally funded projects? YES _____ NO _____

E-verify Status: _____ **Registered:** E-verify Number _____ **DUNS Number** _____
_____ **Not Registered**

Is this contractor/vendor a:

Disadvantaged Business Enterprise under 49 CFR Part 26? YES _____ NO _____

Minority or Women Business Enterprise under 49 CFR Part 23? YES _____ NO _____

Attach a copy of current certification(s).

Is this contractor/vendor a Non-federal entity that expends \$750,000 or more in a year in Federal awards? YES _____ NO _____

If so, attach a copy of most recent single or program-specific audit conducted in accordance with the provisions of OMB Circular A-133.

Certified true and correct:

Name: _____

Signature: _____

Title: _____

Date: _____