







+1 (202) 987 3770 

strongertogether@justiceclimatefund.org 

www.justiceclimatefund.org 

910 17th Street, NW, Suite 820 
Washington, DC 20006

Justice Climate Fund
Request for Proposals (RFP) for Cybersecurity and IT Services

SUMMARY: Justice Climate Fund (JCF) is seeking a qualified Managed Security Service Provider (MSSP) or IT services organization to support JCF’s cybersecurity, IT infrastructure, advanced Microsoft 365 Business Premium support services, and government compliance needs as we scale remote operations to manage a \$940 million federal grant award. JCF invites proposals from firms with expertise in managed security, IT systems, and federal grant compliance.

The selected firm will provide a combination of one-time and ongoing services related to the:

- Design, implementation, and management of cybersecurity systems
- IT systems support and risk mitigation planning
- Compliance with federal cybersecurity requirements
- Microsoft 365 Business Premium advanced support and services
- Training and capacity-building on IT security best practices, anti-phishing and data protection protocols

RFP SUBMISSION INSTRUCTIONS:

All correspondence for this RFP should be directed to: Brenda Loya (bloya@justiceclimatefund.org) Chief Operating and Finance Officer, Justice Climate Fund

Proposals must be submitted electronically in a single .pdf file to: Brenda Loya, bloya@justiceclimatefund.org.

Subject line should read “JCF Cybersecurity and IT Infrastructure RFP” and be submitted electronically by Monday, January 20 by 7:00PM Eastern Time.

REQUEST FOR PROPOSALS SCHEDULE:



Release of Request for Proposals	December 23, 2024
Deadline for Submission of Questions	December 30, 2024
Deadline for JCF to Respond to Questions	January 3, 2024
Submission of Proposals (date and time)	January 23, 2025, by 7:00PM Eastern Time
Announcement of Selections	January 31, 2025
Anticipated Contract Start Date	February 3, 2025
Anticipated Contract End Date	January 1, 2031

ORGANIZATION DESCRIPTION

[JCF](#) is a nonprofit financial institution created to scale the nationwide deployment of affordable, equitable clean energy improvements for disadvantaged American families, businesses, and communities. JCF achieves its mission by enabling and deploying capital through America’s Main Street financial institutions — the very community lenders that have delivered, for decades, financial opportunity, security, and prosperity to struggling Americans. JCF’s network of community lenders pioneered community-based lending. By focusing on communities, JCF will enable American families, communities, and businesses to save money and deliver a greener, cleaner, safer, and more inclusive future for us all. Through the CCIA program, JCF will equip community lenders with new skills, tools, and relationships to successfully deploy affordable, responsible green lending in communities across the country, especially those that are low-income and disadvantaged.

CLEAN COMMUNITIES INVESTMENT ACCELERATOR PROGRAM (CCIA)

Under the \$6 billion Clean Communities Investment Accelerator, JCF (along with four other selected applicants) will establish hubs that provide funding and technical assistance to community lenders working in low-income and disadvantaged communities, providing an immediate pathway to deploy projects in those communities while also building the capacity of hundreds of community lenders to finance projects for years. Each of the selectees will provide capitalization funding (typically up to \$10 million per community lender), technical assistance sub-awards (typically up to \$1 million per community lender), and technical assistance services so that community lenders can provide financial assistance to deploy distributed energy, net-zero buildings, and zero-emissions transportation projects where they are needed most. 100% of capital under the CCIA is dedicated to low-income and disadvantaged communities. [Justice Climate Fund was selected for a \\$940 million award](#) to provide responsible, clean energy-focused capital and capacity building to community lenders across the country.

SCOPE OF WORK

JCF is a fully remote organization with a current headcount of 15 full-time employees (FTEs), projected to expand to approximately 40 FTEs over the next six years. The organization is also supported by a mix of part-time and full-time contractors. Our IT infrastructure is entirely cloud-based, with no on-premises systems or physical server environments. This remote-first model requires a robust, scalable, and secure IT framework to support our operations, collaboration, and data management needs as we grow.

We rely exclusively on the Microsoft 365 cloud ecosystem, leveraging over 20 Business Premium licenses to facilitate key workflows through tools such as Outlook for email communication, Teams for virtual collaboration and meetings, and SharePoint for secure file sharing and document management. The organization requires a comprehensive approach to cybersecurity and IT management to ensure



these tools are optimized for performance, reliability, and compliance with federal grant requirements, including NIST 800-53 standards.

Our primary goal is to partner with an experienced Microsoft Cloud Solutions Provider (CSP) capable of managing and enhancing our existing Microsoft 365 infrastructure. This includes proactive system monitoring, user account management, and the implementation of advanced security measures such as multifactor authentication (MFA), data loss prevention (DLP), and mobile device management (MDM). Additionally, we seek expertise in designing scalable solutions to accommodate anticipated growth, ensuring seamless onboarding for new users and maintaining system integrity as the organization expands. This partnership should also focus on identifying opportunities to integrate advanced Microsoft tools and features that maximize efficiency, foster secure collaboration, and ensure alignment with both organizational goals and federal cybersecurity compliance standards.

The selected firm will support JCF's IT and cybersecurity infrastructure needs, focusing on, but not limited to:

1. Cybersecurity Infrastructure Design and Implementation

- a. Develop and implement a comprehensive cybersecurity strategy tailored to align with federal and EPA requirements, including adherence to the NIST 800-53 framework.
- b. Implement advanced security solutions, including next-generation firewalls, endpoint detection and response (EDR) systems, and secure access service edge (SASE) technologies, to ensure robust threat prevention and protection across remote and cloud-based environments. These tools will integrate with centralized SIEM platforms, enabling real-time monitoring, threat intelligence, and compliance with federal standards.

2. IT Systems Evaluation, Management, and Support

- a. Conduct comprehensive assessments of existing IT systems to identify inefficiencies and vulnerabilities, implementing improvements to enhance performance, scalability, and compliance with cybersecurity frameworks such as NIST 800-53. This includes fine-tuning configurations, optimizing resource allocation, and ensuring alignment with organizational growth and operational needs.
- b. Deliver continuous network monitoring, proactive support for cloud-based IT infrastructure, and the deployment of robust user authentication systems such as multifactor authentication (MFA) and single sign-on (SSO) to safeguard access. Ensure seamless integration of these systems with existing tools while maintaining a secure, user-friendly environment for remote operations.

3. Federal Cybersecurity Compliance

- a. Ensure IT systems adhere to federal cybersecurity frameworks, including NIST 800-53, EPA guidelines, and 2 CFR 200, by implementing comprehensive controls and processes. Prepare systems for annual audits, maintaining detailed documentation to support A-133 and federal grant compliance requirements.

4. Training and Capacity Building



- a. Develop comprehensive cybersecurity manuals and provide targeted training for staff, Board members, and coalition partners to enhance awareness of cybersecurity threats, best practices, and compliance requirements.
- b. Configure, monitor, and manage Microsoft tools to strengthen defenses against spam and phishing attacks, ensuring users are equipped with the knowledge to identify and mitigate risks.
- c. Implement accessible, on-demand training modules tailored to varying levels of technical expertise, enabling ongoing education and skill-building across the organization.

5. Incident Response and Risk Management

- a. Design and implement a detailed Incident Response Plan (IRP) in alignment with NIST SP 800-61 guidelines. This plan will define clear procedures for detecting, reporting, analyzing, and responding to cybersecurity incidents. It will outline roles and responsibilities, communication strategies, escalation paths, and recovery processes to ensure swift and effective action during security events.
- b. Conduct thorough risk assessments to identify and evaluate potential threats, vulnerabilities, and the impact on organizational assets. Establish an ongoing vulnerability management program that includes regular vulnerability scanning, penetration testing, and security assessments. Implement automated patch management processes and remediation strategies to address identified vulnerabilities promptly, reducing risk exposure and enhancing overall security posture.

6. Laptop and Mobile Device Management

- a. Develop and enforce a comprehensive policy for managing personal and company-issued devices, ensuring secure access, compliance with organizational standards, and alignment with cybersecurity best practices.

7. Comprehensive Data Protection Services

- a. Implement, monitor, and manage Microsoft 365 data protection features, including backups, data archiving, retention policies, and governance frameworks. Establish data loss prevention (DLP) measures to safeguard sensitive information and ensure compliance with organizational and regulatory standards.

8. Advanced Microsoft 365 Support Services

- a. Provide advanced support for the Microsoft 365 environment, offering expert guidance on best practices, configuration optimization, and system management. Manage help desk tickets, resolve escalated issues, and coordinate with the Microsoft Support Team for complex problem resolution.

BUDGET

- We do not have a firm budget for this scope of work and look forward to the market helping to inform us of the cost estimate.
- We plan to issue one award to one organization, and we are open to different billing structures, including fixed price, cost reimbursement (with profit margin negotiated), and time and materials.



Justice Climate Fund

- If cost reimbursement or time and materials methodology is chosen, please provide a detailed build-up of your proposed cost.
- Budget will be subject to terms and conditions negotiated with EPA.

PROPOSAL MATERIALS

Responses should include:

1. Cover Letter – Should include the name, title, address, telephone number, and e-mail address for point of contact for the respondent organization on company letterhead.
2. Qualifications – Should include the contractor’s qualifications to conduct the scope of work activities, expertise, knowledge, and experience. Experience should include examples of conducting similar or related work.
3. Project Approach – Should include a narrative of contractor’s proposed approach, including:
 - a. The process and specific activities to be conducted to achieve the stated goals.
 - b. A timeline for the activities.
 - c. Milestones and a detailed list of deliverables tied to activities.
 - d. A detailed budget for each task, along with a proposed payment schedule tied to project milestones or deliverables (if applicable).
 - e. Project Budget – detailed submission and/or labor rate or price listing of all rates for all individuals who will work on the project (if applicable).
4. Engagement Team – resumes and bios for each individual on the specific engagement team we will be working with on a day-to-day basis, including information about experience with similar projects and professional qualifications.
5. Approach to the diversity of the engagement team specifically and, more generally, whether any disadvantaged business enterprise (“DBE”) will be subcontracted as part of your approach to fulfilling our scope requirements. We would also like to see any commitments the firm has to justice, equity and inclusion, including information on diversity training, supplier diversity programs, pro-bono and/or charitable contribution commitments.
6. References – Attach current contact information of clients for whom similar services were provided based on the past projects identified in the qualification form. Please provide at least two references.
7. Disclosure and Certifications
 - a. Indicate whether you are presently engaged or plan to be engaged with any other recipient of Greenhouse Gas Reduction Fund dollars;
 - b. Conflicts of Interest Statement (see below section on Conflicts of Interest);
 - c. Lobbying Certification (see below section on Byrd Anti-Lobbying Amendment).
 - d. Partner Demographics Questionnaire

SELECTION CRITERIA

Criteria	Max Points
<p>MANDATORY CRITERIA: Proposals will not be considered for evaluation without meeting all of the following mandatory criteria:</p> <p>A. The proposer must hold relevant certifications such as CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager), or equivalent industry-recognized credentials.</p>	<p>25</p>



<p>B. Independent. C. No record of substandard work.</p>	
<p>TECHNICAL CRITERIA: Those proposers who have met each of the criteria above will be evaluated on the following criteria:</p> <p>A. Responsiveness of the proposal in clearly stating an understanding of the work to be performed.</p> <ol style="list-style-type: none"> 1. Comprehensiveness of the services to be performed/ scope of work. 2. The proposer has prior experience working on similar projects. 3. The proposer has prior experience working with similar organizations. 4. Quality of submitted work samples. <p>B. Firm's technical experience.</p> <ol style="list-style-type: none"> 1. Demonstrated experience implementing cybersecurity and IT solutions that meet federal grant compliance frameworks with nonprofit organizations (e.g., NIST 800-53, 2 CFR 200). 2. Demonstrates an understanding of the project objectives and desired results. 3. Illustrates an approach to the scope of work that will likely lead to successful results. 4. Illustrates the contractor's ability to successfully execute the proposed approach. 5. Details project activities and milestones, or deliverables, associated with each stage of the scope of work. 6. The work can be completed within the required project timeline. <p>C. Qualifications of proposed staff.</p> <ol style="list-style-type: none"> 1. Qualifications of supervisory personnel. 2. Experience auditing agencies of the type under consideration. 3. Experience auditing similar entities. <p>D. Firm's quality control program.</p> <ol style="list-style-type: none"> 1. The firm must have a robust internal quality control system aligned with federal cybersecurity frameworks (e.g., NIST 800-53) and demonstrate a positive track record through independent third-party assessments, such as penetration testing, SOC 2 audits, or ISO 27001 certification. <p>E. Firm's commitment to justice and equity Evidence of firm or individual commitment to justice and equity through demonstration of diversity plans, past performance with diverse businesses, and commitments to diversity and inclusion initiatives.</p>	<p>50</p>
<p>COST CRITERIA: Reasonableness of proposed audit cost (considering hourly billing rates, number of audit hours, out-of-pocket expenses, and total proposed cost).</p> <ol style="list-style-type: none"> A. The proposal includes a detailed budget for each stage of the scope of work. B. The proposed costs are reasonable. C. The proposed changes to JCF's standard contract terms and conditions are acceptable. 	<p>25</p>
<p>Total Points (max)</p>	<p>100</p>



**ATTACHMENT A - REQUIRED TERMS AND CONDITIONS FOR CONTRACTS SUPPORTED BY
FEDERAL FUNDS**

The following terms and conditions are required to be included in any contract(s) awarded as a result of this solicitation that are supported by federal funds, in whole or in part, during the life of the contract(s). As used herein, “Contractor” shall refer to the selected Proposer and “contracting entity” shall refer to JCF.

BUY USA - DOMESTIC PREFERENCE FOR PROCUREMENTS

1. Contractor should, to the greatest extent practicable under a Federal award, provide a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States (including but not limited to iron, aluminum, steel, cement, and other manufactured products). The requirements of this section must be included in all subawards including all contracts and purchase orders for work or products under this award.
2. For purposes of this section:
 - a. “Produced in the United States” means, for iron and steel products, that all manufacturing processes, from the initial melting stage through the application of coatings, occurred in the United States.
 - b. “Manufactured products” means items and construction materials composed in whole or in part of non-ferrous metals such as aluminum; plastics and polymer-based products such as polyvinyl chloride pipe; aggregates such as concrete; glass, including optical fiber; and lumber.

YRD ANTI-LOBBYING AMENDMENT, 31 U.S.C. § 1352 (AS AMENDED)

Contractors that apply or bid for an award exceeding \$100,000 shall file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or firm for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant, or any other award covered by 31 U.S.C. § 1352. Each tier must also disclose any lobbying with non-Federal funds that takes place in connection with



obtaining any Federal award. Such disclosures are forwarded from tier to tier, up to the non-Federal award.

CLEAN AIR ACT AND WATER POLLUTIONS CONTROL ACT PROVISIONS

Contractor agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Federal Clean Air Act, as amended (42 U.S.C. § 7401 et seq.), and the Federal Water Pollution Control Act, as amended (33 U.S.C. § 1251 et seq.) Contractor agrees to report each violation to the contracting entity and understands and agrees that the contracting entity will, in turn, report each violation as required to assure notification to the grantor federal agency and the appropriate Environmental Protection Agency Regional Office. Contractor agrees to include these requirements in each subcontract exceeding \$150,000 financed in whole or in part with federal assistance.

CONTRACT WORK HOURS AND SAFETY STANDARDS ACT (FOR ANY CONTRACTS IN EXCESS OF \$100,000 WHEN LABORERS OR MECHANICS ARE USED)

1. *Overtime requirements:* No Contractor or subcontractor contracting for any part of the contract work which may require or involve the employment of laborers or mechanics shall require or permit any such laborer or mechanic, in any workweek in which he or she is employed on that work, to work more than forty hours in such a workweek unless such laborer or mechanic receives compensation at a rate not less than one and one-half times the basic rate of pay for all hours worked in excess of forty hours in such a workweek.
2. *Violation: liability for unpaid wages; liquidated damages.* In the event of any violation of the clause set forth in paragraph (1) of this section, Contractor and any subcontractor responsible therefor shall be liable to the affected employee for the unpaid wages. In addition, such Contractor and subcontractor shall be liable to the United States (in the case of work done under contract for the District of Columbia or a territory, to such District or to such territory) for liquidated damages. Such liquidated damages shall be computed with respect to each individual laborer or mechanic employed in violation of the clause set forth in paragraph (1) of this section, in the sum of \$10 for each calendar day on which such individual was required or permitted to work in excess of the standard workweek of forty hours without payment of the overtime wages required by the clause set forth in paragraph (1) of this section.
3. *Withholding for unpaid wages and liquidated damages.* The contracting entity shall upon its own action or upon written request of an authorized representative of the Department of Labor withhold or cause to be withheld, from any moneys payable on account of work performed by Contractor or subcontractor under any such contract or any other federal contract with the same Contractor, or any other federally-assisted contract subject to the Contract Work Hours and Safety Standards Act, which is held by the same Contractor, such sums as may be determined to be necessary to satisfy any liabilities of such Contractor or subcontractor for unpaid wages and liquidated damages as provided in the clause set forth in paragraph (2) of this section.
4. *Subcontracts.* Contractor or subcontractor shall insert in any subcontracts the clauses set forth in paragraphs (1) through (4) of this section and also a clause requiring the subcontractors to include these clauses in any lower-tier subcontracts. The prime Contractor shall be responsible for compliance by any subcontractor or lower-tier subcontractor with the clauses set forth in paragraphs (1) through (4) of this section.

COPYRIGHT AND DATA RIGHTS (IF APPLICABLE)

1. Data, as used herein, shall include any work subject to copyright under 17 U.S.C. § 102, for example, any written reports or literary works, software and/or source code, music, choreography, pictures or images, graphics, sculptures, videos, motion pictures or other audiovisual works, sound and/or video recordings, and architectural works.



Justice Climate Fund

2. Contractor grants to the contracting entity, a paid-up, royalty-free, nonexclusive, irrevocable, worldwide license in data first produced in the performance of this contract to reproduce, publish, or otherwise use, including prepare derivative works, distribute copies to the public, and perform publicly and display publicly such data.
3. For data required by the contract but not first produced in the performance of this contract, Contractor will identify such data and grant to the contracting entity or acquires on its behalf a license of the same scope as for data first produced in the performance of this contract.
4. Upon or before the completion of this contract, Contractor will deliver to the contracting entity data first produced in the performance of this contract and data required by the contract but not first produced in the performance of this contract in formats acceptable by the contracting entity.

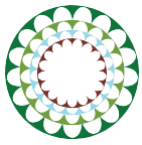
FEDERAL COMPLIANCE

Contractor acknowledges that Federal funds will be used to fund all or a portion of the contract. Contractor will comply with all applicable Federal law, regulations, executive orders, policies, procedures, and directives. This specifically includes, *but is not limited to*, all 2 CFR 200 requirements, and any Inflation Reduction Act (IRA) requirements and guidance established by the United States Department of the Treasury and/or the EPA for IRA funding. It also includes any legal requirements applicable to the Bipartisan Infrastructure Law, Greenhouse Gas Reduction Fund, and Urban Area Security Initiative (UASI) funding.

PROHIBITION ON CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (HUAWEI AND ZTE) (IF APPLICABLE)

Contractor and any sub-contractor are each prohibited from obligating or expending loan or grant funds to:

1. Procure or obtain;
 2. Extend or renew a contract to procure or obtain; or
 3. Enter into a contract (or extend or renew a contract) to procure or obtain equipment, services, or systems that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. As described in Public Law 115–232, section 889, covered telecommunications equipment is telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities).
- (1) For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities).
- (2) Telecommunications or video surveillance services provided by such entities or using such equipment.
- (3) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.



PUBLICATIONS CLAUSE (FOR INFLATION REDUCTION ACT “IRA” FUNDS)

Any publications produced with funds from this award must display the following language: “This project [is being] [was] supported, in whole or in part, by federal award number [enter project FAIN] awarded to [name of Recipient] by the U.S. Department of the Treasury.” This requirement is subject to change based on the requirements of EPA.

RIGHTS TO INVENTIONS MADE UNDER A CONTRACT OR AGREEMENT (IF APPLICABLE)

Contracts or agreements for the substitution of parties, assignment, or performance of experimental, developmental, or research work shall provide for the rights of the Federal Government and the recipient in any resulting invention in accordance with 37 CFR part 401, “Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements,” and any applicable implementing regulations.

SUSPENSION OR DEBARMENT

1. No contract will be awarded to a Contractor or any party that is debarred from working on federally funded projects, as listed on the government-wide exclusions list in the System for Award Management (SAM) at www.sam.gov, in accordance with the OMB guidelines at 2 C.F.R. Part 180.
2. This contract is a covered transaction for purposes of 2 C.F.R. Part 180 and 2 C.F.R. Part 3000. As such, Contractor is required to verify that none of Contractor’s principals (defined at 2 C.F.R. § 180.995) or its affiliates (defined at 2 C.F.R. § 180.905) are excluded (defined at 2 C.F.R. § 180.940) or disqualified (defined at 2 C.F.R. § 180.935).
3. The bidder or proposer agrees to comply with the requirements of 2 C.F.R. Part 180, subpart C and 2 C.F.R. Part 3000, subpart C while this offer is valid and throughout the period of any contract that may arise from this offer.

AUDITS

The sub-recipient must submit the audit to the recipient within 9 months of the end of the recipient’s fiscal year or 30 days after receiving the report from an independent auditor, whichever is earlier. As provided in 2 CFR 200.337(a) the recipient must provide EPA, the EPA Office of Inspector General, and the Comptroller General with access to the subrecipient’s independent auditor reports.

[Signature Page Follows]



ACKNOWLEDGMENT AND CERTIFICATION:

On behalf of [NAME OF FIRM], I hereby:

1. Acknowledge that the specific terms and conditions outlined in this Attachment A will be fully incorporated into any contract(s) awarded as a result of this solicitation that are supported by Federal funds, in whole or in part, during the life of the contract(s); and
2. Commit to adhere to all relevant regulations, guidelines, and requirements outlined in this RFP and all Attachments contained within this RFP. Compliance with these regulations is crucial for maintaining the integrity of the qualification process and ensuring fair evaluation.

Name of Firm:

Name of Individual:

Title:

Signature: _____

Date:

SIGN AND RETURN THIS FORM WITH YOUR PROPOSAL SUBMISSION

- a) Promptly notify JCF in writing of any legal proceedings resulting from any subcontract or other commitment related to the terminated portion of the contract;
- b) Settle outstanding liabilities and proposals arising out of the termination; and
- c) If there is a terminated construction contract, ensure the cleanup of the site, protection of serviceable materials, removal of hazards, and other actions necessary to leave a safe and healthful site.

[END OF DOCUMENT]