IOLA Fund of the State of New York

Justice Infrastructure Project:
Technology Consultant Services

Application Process Questions & Answers
(FINAL as of April 15, 2024)

RFP Process

Question 1: Is IOLA available to meet with us to discuss the RFP?

Answer: IOLA cannot meet with any applicants regarding an open RFP. All questions should be submitted in writing via email on or before 4:00 pm, Wednesday, April 10, 2024. Answers will be posted publicly by April 17, 2024.

Question 2: Will IOLA select more than one company to perform the scope of work?

Answer: IOLA anticipates selecting one vendor.

Question 3: Can a company bid on only select items? E.g. just the phishing/training awareness or policy development

Answer: IOLA seeks a vendor to address the entire scope of services set out in the RFP.

Question 4: Do you expect the vendor to provide a costing proposal for one or 25 grantee organizations?

Answer: IOLA expects the vendor to provide a proposal to support at least 15 grantee organizations.

Question 5: Depending on our assessment, we will provide recommendations on deploying specific security tools. How do you want us to respond the questions related to Software and Licensing cost?

Answer: Provide your best estimate of software and licensing costs that you think are most likely to be used.

Question 6: As per RFP page 6, under Required Documents Tab, what do we need to submit for Work Samples from Similar Projects. Do we need to submit work sample of organization or proposed team members?

Answer: Submit work samples of the organization and/or of the proposed team members that are most relevant to IOLA’s Project.

Question 7: What level of candidates are required by the agency for this project? Could the agency clarify the positions and their job descriptions required for this project? Are there any preferred certifications needed for resources?

Answer: No minimum level of candidates or certifications are required, but relevant expertise and experience is a factor in our evaluation of bids. As stated in the RFP, applications will be evaluated on the following criteria: Organizational Capacity, Relevant Expertise & Experience, Service Quality, & Project Budget. IOLA will utilize a “Best Value” selection process to ensure optimum quality, cost, and efficiently among responsive and responsible applicants.

Question 8: Is it mandatory to having expertise with civil services aid for bidding on this opportunity?

Answer: It is not mandatory to have expertise with civil legal services aid in order to bid on this opportunity, but relevant expertise and experience is a factor in our evaluation of bids. As stated in the RFP, applications will be evaluated on the following criteria: Organizational Capacity, Relevant Expertise & Experience, Service Quality, & Project Budget. IOLA will utilize a "Best Value" selection process to ensure optimum quality, cost, and efficiently among responsive and responsible applicants.

Question 9: Is there any page limit for this bid?

Answer: There is no page limit for this bid.

Question 10: Who will be responsible for procuring the necessary software and hardware – the consultant or the grantees? And how should this be factored into the budget?

Answer: Software and hardware improvements/upgrade costs will be borne by the grantees. Provide your best estimate of software and licensing costs that you think are most likely to be used in the project workplan. These should not be included in the Project Budget. See also Question 5 & Question 12.

Question 11: For the interim and final reports, are there specific formats, templates, or key elements that IOLA expects to be included? How detailed should the observations and recommendations be, and is there a preference for the structure of these reports? Is there any specific information or analysis that should be included?

Answer: IOLA will work with the vendor on appropriate formats for interim and final reports. These reports may include, but would not be limited to, information about the process the vendor undertook, the methodologies it used, any research it performed, feedback it received from grantees during its work, notable challenges or obstacles to completion of the work, and the basis for the vendors recommendations. The observations and recommendations should be sufficiently detailed for IOLA to understand the basis for the observations and recommendations and for IOLA to take reasonable steps to act on them.

Contract Administration

Question 12: Regarding the “Implement any recommended upgrades, transitions, and/or improvements” requirement in Section C. Scope of Services, will the vendor perform the implementation services or will the vendor provide support for the implementation?

Answer: IOLA grantees are independently operated non-profit organizations. The vendor will be assisting grantees with appropriate cybersecurity upgrades, transitions, and/or improvements.

Question 13: What is the timeline expected for this project?

Answer: The term of the contract is for one year, with the possibility to renew the contract and amend the scope of services.

Question 14: Do the grantees currently have an in-house or outsourced IT department? What is the current infrastructure of the IOLA Grantees to support adoption of cyber security and/or supporting technologies?

Answer: IOLA grantees are independently operated non-profit organizations. IT support and infrastructure varies among IOLA grantees.

Question 15: Are the grantees located in NYC metro area?

Answer: IOLA grantees are located throughout New York State.

Question 16: Is there an incumbent providing similar services currently and in the prior years? If so, who is the current vendor and what is contract pricing?

Answer: This is a new initiative.

Question 17: The RFP mentions the possibility of renewing the contract to support future Project activities, including improvements to technology infrastructure and development of technology resources. Can you provide examples or potential areas of focus for these future activities?

Answer: The services the technology consultant will provide are part of the larger Justice Infrastructure Project IOLA recently launched in 2023. Consistent with the IOLA Fund's mission, this Project seeks to ensure that every New Yorker with a legal problem has clear and timely access to high quality legal information, advice, and representation.

The Justice Infrastructure Project is expected to evolve over several years and future activities may include:

1) Improvements to other elements of the technology infrastructure of IOLA grantees, especially improvements that will aid with increased data collection and information sharing.
2) Development of technology resources to assist with preventing common civil legal problems and diverting disputes from high volume courts.

Question 18: How does IOLA envision the consultant's interaction with grantees throughout the project? Are there established communication protocols or platforms for collaboration?

Answer: IOLA grantees are independently operated non-profit organizations with varying communication methods and systems. Microsoft Teams is common among grantees but is not uniformly used.

Question 19: What level of involvement should the consultant expect from IOLA’s team during the project? Will there be a dedicated point of contact or oversight committee?

Answer: IOLA has contracted with Stout Risius Ross to serve as the overall Justice Infrastructure Project project manager. Stout and IOLA staff will oversee the vendor.

Question 20: Do we need to submit COI along with proposal or shall we submit it after award?

Answer: The vendor will be required to submit proof of current insurance coverage as part of the contract execution process.

Question 21: Can you share the estimated budget per grantee or the total budget you have allocated for this RFP?

Answer: The total project budget has yet to be determined, but is expected not to exceed $250,000 (excluding software and licensing costs that will be borne by IOLA grantees).

Question 22: How does IOLA define success for this project, and are there specific metrics or outcomes you aim to achieve?

Answer: IOLA recognizes that this project may be approached in different ways and specific outcomes will be developed with the successful vendor.

Question 23: Is there flexibility in the project timeline, especially considering the varying capabilities of grantees to implement changes?

Answer: This has not been determined.

Question 24: Could you elaborate on the conditions under which the contract might be renewed after the initial term?

Answer: This has not been determined.

Question 25: Do all resources need to be located within the United States? Will offshore or near shore consultants be allowed access to the systems?

Answer: Please see Appendix A: Standard Clauses for New York State Contracts: https://ogs.ny.gov/procurement/appendix

Question 26: Our assumption is that resources can work remotely for tasks that do not require an onsite presence. Could you please confirm?

Answer: Yes, virtual service is permitted.

Question 27: What email tool is used by IOLA?

Answer: The IOLA Fund uses Microsoft Outlook as its primary email tool, however, email tools used by grantees vary.

Scope of Services

Question 28: Is the scope listed accurate? Is the RFP currently primarily targeted to cyber security architecture?

Answer: The RFP targets the cybersecurity needs of IOLA’s grantees, including identifying, implementing, and providing training on cybersecurity improvements.

Question 29: Can you elaborate on the expectations regarding data security and privacy, especially in relation to sensitive legal information handled by IOLA grantees? Are there specific legal or regulatory compliance requirements (e.g., data protection laws) that the grantees need to meet through the security enhancements?

Answer: IOLA grantees provide legal services and, therefore, typically possess confidential and privileged client information that must be protected.

Question 30: Are there specific milestone dates that are targeted to have this work (the four areas to be addressed per the RFP) completed for the 15-25 IOLA Grantees (i.e. depending on the current technology maturity of the organization, there may be remediation required prior to the adoption of cyber security controls)?

Answer: IOLA will look to the vendor for recommendations on specific milestone dates for grantees.

Question 31: How would you like the consultant to handle change management and stakeholder communication during the implementation of technology enhancements?

Answer: IOLA will look to the vendor for recommendations on change management and stakeholder communication.

Question 32: What are IOLA's expectations for post-project support from the consultant, especially regarding maintenance and updates to the implemented technologies?

Answer: IOLA will look to the vendor for recommendations on post-project support, maintenance, and upgrades.

Question 33: What is the expectation for the grantees that are in need of enhanced security but do not have the necessary time and resources to improve policies, procedures, and technologies?

Answer: IOLA expects the vendor to identify and assist grantees that are both a) in need of enhanced security and b) have the necessary time and resources to improve policies, procedures, and technologies. The vendor is expected to assist 15-25 of IOLA's 80 grantees.

Technology Infrastructure, Practices, and Policies of IOLA Grantees

Question 34a-34s:

a. Who are IOLA Grantees?
b. What existing information security policies are currently in place within the grantee organizations?
c. Do the grantees have email incident response processes in place?
d. Has there been a past risk assessment to identify where policies, standards, and procedures are missing or lacking to address the needs?
e. Is there a current phishing and awareness training platform in place? If so, can it be used for this endeavor?
f. What are the size and technical structure of the grantee organizations? Including the number of users, devices, on-premises apps, cloud applications, etc.
g. What are the email systems in use by the grantees, e.g., Office 365, Google Workspace, Exchange on-premises, etc.?
h. Can you provide a list of equipment? How many devices are in use?
i. Do the grantees have the necessary resources and staff to support the consultant? Do the grantees have staff to respond to interviews/questionnaires? Do the grantees have the budget to make the necessary enhancements/changes needed to improve their security. What are the limitations or constraints?
j. What is the current infrastructure of the IOLA Grantees to support adoption of cyber security and/or supporting

technologies?

k. What are the demographics of IOLA Grantee organizations including: Number of employees, Location, Avg Annual Revenue
l. Should each grantee be treated as its own company with its own infrastructure (including cloud infrastructure)?
m. What is the current IT infrastructure model being used? On-Premises, Cloud, Hybrid? If it is Cloud or Hybrid, which Cloud service provider is being used?
n. Which Identity Service Provider is being used?
o. What Email Security policies have been implemented at a high level?
p. Can you provide more detailed profiles of the IOLA grantees, including their sizes, the nature of their current technology infrastructure, and any known cybersecurity concerns?
q. Have any of the grantees undergone previous technology or security assessments, and can the results of these assessments be shared?
r. What types of cybersecurity training have the grantees received in the past, and were there any identified gaps or areas for improvement?
s. To assist in bidding, can we get a specific number of organizations? Along with: number of staff per organization, number of sites for each organization, if the organization uses Microsoft 365, Google Workspace or both or neither, if the organization uses on-premises servers (Windows, Apple or Other), if the organization is predominantly Windows-based or uses other devices/platforms

Answer: IOLA grantees are independently operated non-profit organizations located across New York State providing civil legal services to low-income and other eligible people.

IOLA grantees vary from approximately 5 to 640 FTE staff, with an approximate average of 68 FTE staff. For additional information, https://www.iola.org/grantees/about-iola-grantees

Existing technology and security practices, equipment, systems and software, infrastructure, IT support, and technological capacity vary from organization to organization.

The New York State Permanent Commission on Access to Justice conducted technology surveys in 2013, 2018, and 2023. Survey information may be available on the NYS Unified Court System website: https://ww2.nycourts.gov/accesstojusticecommission/tsurvey.shtml

Additionally, IOLA is currently conducting a short survey of grantees focused on cybersecurity practices and policies, the results of which will be shared with the vendor.

IOLA will look to the vendor for recommendations regarding which grantees are a) in need of enhanced security and b) have the necessary time and resources to improve policies, procedures, and technologies.

Question 35a-35w:

a. How many and what type of policies need to be developed?
b. Is there a particular cybersecurity framework or control set adopted that has guided any past policy development?
c. Are there cyber liability insurance policy requirements that would serve as a baseline for an assessment?
d. How many people need to be subject to a phishing campaign and how many campaigns are expected? Will automated training based on phishing activities meet the training requirements?
e. Regarding training, what are the specific technology security needs of the providers? Are there specific areas within email security, multifactor authentication, phishing training, and cybersecurity policy development that are of particular concern or priority?

f. Which solutions are expected to be designed and deployed under the scope of email security, e.g., phishing protection, link protection, malware protection, data leak protection, email encryption?

g. In the goal of efficiency, are graymail management systems reasonable to also offer for deployment?

h. Regarding MFA/SSO requirements, what systems are they planned for (e.g. on premise applications, windows servers, Linux servers, user workstations, Office 365/Google Workspace)? Furthermore is this planned for extending to public-facing sites/applications?

i. For the project workplan - do you anticipate any specific software or systems that needs to be deployed?

j. Regarding the review of technology and security practices of current IOLA grantees, are there standardized benchmarks or compliance standards that grantees are expected to meet, or do you expect the awardee to recommend the standards?

k. How will IOLA determine which grantees are "in need of enhanced security"? Can you explain what enhanced security implies?

l. Could you elaborate on the types of training specific to grantees' needs? Are there certain thematic areas or common challenges anticipated that the training should focus on?

m. The RFP mentions directly assisting 15-25 IOLA grantees. Can you provide more context on what this assistance entails? Does it include hands-on technical implementation, advisory services, or both?

n. Are there preferred or existing technology stacks and platforms among the IOLA grantees that the consultant should be aware of or proficient in? How important is the integration and compatibility of new cybersecurity measures with existing systems and software used by IOLA grantees? Are there any known constraints?

o. Are there any phishing campaign tools that we can use or should we provide the phishing campaign tool?

p. Are we expected to create contents for the phishing awareness purposes?

q. How many phishing campaigns are expected to be run for this project?

r. Is there a preference or requirement for standardizing security measures across grantees versus tailoring solutions to each organization's unique needs?

s. What formats of training (e.g., in-person, virtual, self-paced) do you believe will be most effective for the grantees?

t. The RFP to “review the technology and security practices of current IOLA grantees”. What is the expected scope of this review and is there a recognized compliance standard to use in the review? Typical scope items that come to mind include the following: review of users’ computers, review of physical security through onsite assessment, network and firewall internal and external “blue team/red team” penetration testing, simulated social engineering and phish testing, Microsoft 365 and/or Google platform review (security and recommended features) Are the above good scope items? Are any not desired? Are there any not listed that you would like to include?

u. Pricing for security assessment can vary depending on whether the assessment organization directly verifies all information (more effective), or relies on user self-reporting and checklist (less costly). Which level of verification is desired in this scenario?

v. Email Security can cover several items, including: MFA protection, attachment sandboxing, real-time link detection, SPF/DMARC/DKIM verification, etc., conditional access to automatically block access from out-of-country, legacy authentication, insecure protocols, access from unauthorized devices and so on, unless added to a specific exception group for a limited time, Digital Loss Prevention (no auto-forwarding to personal email, PII must be encrypted, etc.), setting up ways to share protected and sensitive information so emailing PII isn’t required. Are configurations for email security above and beyond MFA-only protection desired?

w. Training, in addition to Security Awareness Training (SAT), can take many forms. Are there scope requirements for this deliverable? Examples include: live webinars for each organization each month (or quarter), live webinars for all organizations each month (or quarter), basic IT skills assessment and training on Windows, iOS, MS Office and other products through a Learning Management System (LMS), or all of the above.

Answer: IOLA grantees are independently operated non-profit organizations.

The Legal Services Corporation (LSC) released “LSC Baselines: Technologies That Should Be in Place in a Legal Office Today (Revised 2023)” that offers relevant standards to inform how IOLA grantees should operate, but IOLA will look to the vendor for recommendations.

The LSC Baselines report may be available at the LSC website: https://lsc-live.app.box.com/v/LSC-Technology-Baselines

While organizations have varying technology systems, LegalServer is a common case management system among grantees. Microsoft Teams is also widely, but not uniformly used, among grantees. IOLA will look to the vendor for recommendations as to integration and compatibility issues.

The goal of this contract is to deploy a technology consultant to improve the cybersecurity of at least 15 grantees as described in the RFP. How the vendor proposes to accomplish this goal should be described in the project workplan.

Ultimately, IOLA will look to the vendor for recommendations regarding the quantity, quality, and nature of specific technology upgrades, transitions, improvements, trainings, and deployments.