EXHIBIT E
VENDOR DATA SECURITY QUESTIONNAIRE

WHERE NO SOC-2 IS AVAILABLE, PLEASE FILL OUT THE ATTACHED QUESTIONNAIRE.

If selected through this RFP process respondent shall provide an initial security controls assessment in the form attached hereto (**Vendor Data Security Questionnaire**) prior to executing an agreement with LACERA. All subsequent security controls assessments that are required after this first report shall be performed and submitted annually. The answers provided in the questionnaires are to focus on security as it applies to the technologies impacting services provided in relation to the scope of work. If a security control is found to be inadequate, the respondent will develop a remediation plan within 30 days. The respondent will implement the plan and inform LACERA of the change within a mutually agreed upon and reasonable time.

The answers to the Vendor Data Security Questionnaires shall report in writing on the respondent's system(s) and the suitability of the design and operating effectiveness of controls, information functions, and/or processes applicable to the environment in which the respondent receives and maintains LACERA records, including the security requirements.

Respondent shall provide to LACERA, within 30 calendar days of the issuance of each Vendor Data Security Questionnaire, a documented corrective action plan that addresses each audit finding or exception contained therein. The corrective action plan shall show in detail the required remedial action by the respondent along with the implementation date(s) for each remedial action.

If the respondent does not provide a completed annual Vendor Data Security Questionnaire, LACERA shall have the right to retain an independent audit firm to perform such an audit engagement for such a report. The audit will include the controls, information functions, and processes used or provided by the respondent. Respondent agrees to allow the independent audit firm to access its facilities for the purposes of conducting this audit engagement. They will provide the necessary support and cooperation to the independent audit firm.

The independent audit firm will be engaged by LACERA's legal department and subject to the same confidentiality requirements supported in this agreement, and any disclosure will be on a need-to-know basis only for the purpose of the Vendor Data Security Questionnaire. LACERA will invoice the respondent for the expense of the report(s) or deduct the cost from future payments to the respondent.

LACERA

VENDOR DATA SECURITY QUESTIONNAIRE

1. GENERAL INFORMATION

Name of Vendor:Click or tap here to enter text.

Vendor is a(an): ☐Individual ☐Corporation ☐ Partnership ☐Other Click or tap here to enter text.

2. SAFEGAURDS ON LACERA CONFIDENTIAL INFORMATION

a) Does / will the vendor hold LACERA Confidential or LACERA member PII information? ☐Yes ☐No
If yes, please provide details. Response: Click or tap here to enter text.

b) Is LACERA information physically or virtually segregated from the vendor and its vendor's other clients? ☐Yes ☐No
If yes, please provide details. Response: Click or tap here to enter text.

c) Provide brief description on the type of connection (encryption and authentication) for information exchange between LACERA and the vendor organization. Response: Click or tap here to enter text.

d) Is LACERA information encrypted at rest? ☐Yes ☐No

e) Describe the teams within vendor's organization that have access to the LACERA information:
Response: Click or tap here to enter text.

f) Are vendor's production and test/development areas separated? ☐Yes ☐No
If yes, please provide brief details. Response: Click or tap here to enter text.

3. VENDOR Security and INCIDENT RESPONSE PROGRAM

a) Provide documentation on vendor Information Security Policy and Incident Response programs.
Response: Click or tap here to enter text.

b) Provide confirmation and/or attestation to a 72-hour breach notification.
Response: Click or tap here to enter text.

c) Vendor agrees to a periodic review for compliance to LACERA policies and security requirements. ☐Yes ☐No
Response: Click or tap here to enter text.

4. VENDOR PENETRATION TEST AND SOC2 REPORTS

a) Has the vendor completed a Penetration test? ☐Yes ☐No
Provide summary report of the latest Penetration Test. Response: Click or tap here to enter text.

b) Has the vendor completed an Independent Service Auditors compliance exam such as SOC 2? ☐Yes ☐No
If yes, please provide the latest audit report and proceed to the last section of this questionnaire sign and date the document.
Response: Click or tap here to enter text.

If compliance report has not been completed, please proceed to the next sections.

5. EMAIL SECURITY CONTROLS

If the answer to any question in this section is "No", please provide additional details in the "Additional Comments" section.

a) Do you tag external emails to alert employees that the message originated from outside the organization? ☐Yes ☐No

b) Do you pre-screen emails for potentially malicious attachments and links? ☐Yes ☐No
If "Yes", complete the following:
Provide your email security provider. Response: Click or tap here to enter text.
Do you have the capability to automatically detonate and evaluate attachments in a sandbox to determine if they are malicious. ☐Yes ☐No

c) Have you implemented any of the following to protect against phishing messages? (check all that apply):
☐Sender Policy Framework (SPF)
☐DomainKeys Identified Mail (DKIM)
☐Domain-based Message Authentication, Reporting & Conformance (DMARC)
☐None of the above

d) Can your users access email through a web application or a non-corporate device? ☐Yes ☐No
If "Yes", do you enforce Multi-Factor Authentication (MFA)? ☐Yes ☐No

e) Do you use Office 365 in your organization? ☐Yes ☐No
If "Yes", do you use the Office 365 Advanced Threat Protection add-on? ☐Yes ☐No

ADDITIONAL COMMENTS (Use this space to explain any "No" answers in the above section and/or to list other relevant IT security measures you are utilizing that are not listed here.)

Response: Click or tap here to enter text.

6. INTERNAL SECURITY

If the answer to any question in this section is "No", please provide additional details in the "Additional Comments" section.

a) Do you use a cloud provider to store data or host applications? ☐Yes ☐No
If "Yes", provide the name of the cloud provider. Response: Click or tap here to enter text.

b) Do you use MFA to secure all cloud provider services that you utilize (e.g. Microsoft Azure)? ☐Yes ☐No

c) Do you encrypt all sensitive and confidential information? ☐Yes ☐No
If "No", are the following compensating controls in place:
1. Segregation of servers that store sensitive and confidential information? ☐Yes ☐No
2. Access control with role-based assignments? ☐Yes ☐No

d) Do you allow remote access to your network? ☐Yes ☐No
If "Yes", do you use MFA to secure all remote access to your network? ☐Yes ☐No

e) Do you use a next-generation antivirus (NGAV) product to protect all endpoints across your enterprise? ☐Yes ☐No
If "Yes", provide name of your NGAV provider. Response: Click or tap here to enter text.

f) Do you use an endpoint detection and response (EDR) tool that includes monitoring and logging? ☐Yes ☐No
If "Yes", provide name of your EDR provider. Response: Click or tap here to enter text.

g) Do you manage privileged accounts using privileged account management software (PAM) ☐Yes ☐No
If "Yes", provide name of your PAM provider. Response: Click or tap here to enter text.

h) Do you roll out a hardened baseline configuration across servers, laptops, desktops? ☐Yes ☐No

i) Do you record and track all software and hardware assets deployed across your organization? ☐Yes ☐No

j) How frequently do you install critical and high severity patches across your enterprise? ☐Yes ☐No

k) Do you use a protective DNS service (PDNS) to block access to known malicious websites? ☐Yes ☐No

l) Do you implement PowerShell best practices as outlined by Microsoft? ☐Yes ☐No

m) Do you utilize a Security Information and Event Management system (SIEM)? ☐Yes ☐No

n) Do you utilize a Security Operations Center (SOC)? ☐Yes ☐No
If "Yes", complete the following:
Is your SOC monitored 24 hours a day, 7 days a week? ☐Yes ☐No
If your SOC is outsourced, provide name of your SOC provider. Response: Click or tap here to enter text.

o) Do you have an established Third Party Risk Management Program (TPRM)? ☐Yes ☐No

ADDITIONAL COMMENTS (Use this space to explain any "No" answers in the above section and/or to list other relevant IT security measures you are utilizing that are not listed here.)

Response: Click or tap here to enter text.

7. PHISHING CONTROLS

a) Do all employees at your company complete mandatory cybersecurity training? ☐Yes ☐No
If "Yes", does such training include phishing simulation? ☐Yes ☐No

8. BACKUP AND RECOVERY

If the answer to any question in this section is "No", please provide additional details in the "Additional Comments" section.

Do you use a data backup solution? ☐Yes ☐No
If "Yes":

a) Which best describes your data backup solution?
☐Backups are kept locally but separate from your network (offline/air-gapped backup solution).
☐Backups are kept in a dedicated cloud backup service.
☐You use a cloud-syncing service (e.g. Dropbox, OneDrive, SharePoint, Google Drive).

b) Check all that apply:
☐Your backups are encrypted
☐You have immutable backups
☐Your backups are secured with different access credentials from other administrator credentials
☐You utilize MFA for both internal and external access to your backups
☐You have tested the successful restoration and recovery of key server configurations and data from backups
☐You are able to test the integrity of backups prior to restoration to ensure that they are free of malware

c) Estimated amount of time it will take to restore essential functions using backups in the event of a widespread malware or ransomware attack within your network.
☐0-24 hours ☐1-3 days ☐4-6 days ☐1 week or longer

d) Has the vendor completed Disaster Recovery testing? ☐Yes ☐No
If yes, please provide RTO/RPO objectives (Recovery Time Objective or Recovery Point Objectives).
Response: Click or tap here to enter text.

ADDITIONAL COMMENTS (Use this space to explain any "No" answers in the above section and/or to list other relevant IT security measures you are utilizing that are not listed here.)

Response: Click or tap here to enter text.

9. INCIDENTS

a) Has the vendor received any complaints or written demands or been a **subject in litigation** involving matters of privacy injury, breach of private information, network security, defamation, content infringement, identity theft, denial of service attacks, computer virus infections, theft of information, damage to third party networks or the ability of third parties to rely on the vendor's network? ☐Yes ☐No

b) Has the vendor been the subject of any government action, investigation, or other proceedings regarding any alleged violation of privacy law or regulation? ☐Yes ☐No

c) Has the vendor notified customers, clients or any third party of any security breach or privacy breach? ☐Yes ☐No

ADDITIONAL COMMENTS (Use this space to explain any "Yes" answers in the above section.)

Response: Click or tap here to enter text.

10. CERTIFICATION, CONSENT AND SIGNATURE

The vendor has read the foregoing and understands that completion of this questionnaire does not bind LACERA to procure vendor's products or services. I hereby declare that, after inquiry, the above statements and particulars are true, and I have not suppressed or misstated any material fact.

Print or Type Vendor's Name: Click or tap here to enter text. Title of Signee: Click or tap here to enter text.

Signature of Signee: Click or tap here to enter text. Date signed: Click or tap here to enter text.