NEW YORK STATE OF OPPORTUNITY. | Department of Financial Services

Application to be Approved as an Electronic Open Auction Municipal Bond Services Provider

Part I – General Information

Applicant Name:

Business Address:

Mailing Address (if different from your business address):

Applicant's Website:

Name of Person Submitting the Application:

Title:

Telephone Number:

Email Address:

Part II – Experience Providing Bond Auction Services

Describe the Applicant's experience offering bond auction services. Include in your answer when the Applicant started offering bond auction services, a description of the products and services the Applicant has offered through its history, and the experience of the Applicant's key staff in providing bond auction services.

Identify any lawsuits, arbitration or mediation filed against the Applicant in the last ten years that relate to its offering of bond auction services. For each lawsuit, arbitration or mediation so identified, provide the caption and index number for the case, the venue in which the case was filed, and a description of the alleged wrongful conduct and the resolution of the matter, if any.

Identify any governmental investigations relating to the Applicant's offering of bond auction services over the last ten years. For each investigation so identified, state the agency or governmental entity that conducted the investigation, the name and contact information for that entity or agency and provide a description of the nature of the investigation and any resolution thereof.

Part III – Business Model Description

Describe any open auction bidding system that Applicant will offer in New York. For each open auction bidding system, include the following information:

- how potential bidders are alerted to an offering on the system and what documents or information is made available to potential bidders;
- a description of the bidding process;
- how bids are calculated;
- the information available to bidders and issuers during the auction;
- how and when a winner is determined;
- maturity and pricing models;
- all fees can costs charged for using the platform, the amounts, and who the fees or costs are charged to; and
- technical support for anyone using the Applicant's auction system.

Describe how the Applicant determines who it allows to bid in auctions hosted on its system. Include in the description any minimum qualifications that potential bidders must meet, how the Applicant verifies information submitted by potential bidders, and any security posting requirements imposed by the Applicant.

Part IV – Technology and Security Practices

A. General Security

1. Describe how the Applicant authenticates users of the system that hosts the open auction function and include answers to the following:
    a. How do users of the Applicant's system access the auction function?
    b. How does the Applicant issue login credentials?
    c. How does the Applicant verify and authenticate users?
    d. Does the Applicant require multifactor authentication to access its system?
2. Provide documentation and information regarding the Applicant's cybersecurity program, including any cybersecurity policies, risk assessment programs, access control policies, data disposal policies, both with respect to physical access and access to nonpublic information, and any other cybersecurity procedures, guidelines and/or standards the Applicant has established and maintained.
3. Provide a copy of the Applicant's latest cybersecurity risk assessment.
4. If the Applicant has a documented cybersecurity awareness program, please provide it. Has that program that has been approved by management?
5. If the Applicant has a documented information asset protection program, please provide it. Has it been approved by management and communicated to appropriate staff?
6. Does the Applicant require the use of a VPN when users of its information systems access those systems from remote locations?
7. Does the Applicant use encryption when transmitting or receiving confidential and nonpublic information over public networks?

8. If the Applicant has a documented policy for vendor and third party service provider information security risk management, please provide it. How often does the Applicant perform reviews of third parties that have access to its data?

B. Organizational Security

9. Has the Applicant's cybersecurity program been approved by management?
10. Does the Applicant have a Chief Information Security Officer (CISO) or other employee who acts as the central point of contact for cybersecurity? If so, please provide the name of the CISO or the name and title of the employee.
11. Please provide copies of any cybersecurity training that the Applicant's employees, third parties, independent contractors and others who have access to the Applicant's information systems have attended and any logs regarding their attendance.
12. Does the applicant perform background checks on personnel that access and handle confidential and nonpublic information?

C. Business Continuity & Disaster Recovery

13. If the Applicant has a documented policy for business continuity and disaster recovery, please provide it. Has it been approved by management and communicated to the appropriate staff? When was the last successful business continuity and disaster recovery test conducted?

D. Incident Response & Notification

14. Has the Applicant experienced an information security breach in the past five years? If so, please document the nature of the breach, describe how those affected were notified, and explain how soon after the breach occurred did the Applicant notify any affected parties.
15. Does the Applicant collect, review and monitor system logs to detect and respond to anomalies and security incidents?
16. If the Applicant has a documented incident response plan, please provide it. Has it been approved by management and communicated to the Applicant's staff? How often is the incident response plan tested?
17. If the Applicant has Privacy and Network Security insurance (sometimes known as Cyber Liability insurance) covering loss/disclosure of data, system or privacy breach, denial or loss of service, introduction or spread of malicious software code, and unauthorized access/use of computer systems or data, please provide the policy and the coverage limits.

E. Auditing & Reporting

18. Has the Applicant conducted penetration tests or vulnerability assessments? Did these tests and assessments reveal any material gaps in the Applicant's cybersecurity? If so, please provide a list of gaps and any remedial efforts the Applicant is undertaking to address the deficiencies.
19. Does the Applicant have or maintain an SSAE-18 SOC report or documented cybersecurity audit and compliance program that has been approved by management? If so, please document which type of report is being maintained and provide a copy of the latest report.

Questions about the Bond Services Provider Application or application process should be directed to this department at BondServicesProvider@dfs.ny.gov.