NYSIF

PO BOX 66699; ALBANY, NY 12206
518.437.4360 | **nysif.com**

September 7, 2023

The following (Q&A) will serve as Amendment #1 to NYSIF's Invitation for Bids (IFB) for Payment Card Industry (PCI) Compliance Testing, bid number 2023-43-INS. Material in this Amendment supersedes any contradictory material in the IFB.

Please note that the due date for the submission of bids remains the same.

All bids are due 9/15/23, by 2:00 p.m. (Eastern).

Sincerely,

Melissa McClellan

Melissa McClellan
Contract Management Specialist 2

Payment Card Industry (PCI) Compliance Testing
IFB 2023-43-INS
Amendment 1

Question #	IFB Page #	IFB Section and Sub-Section Reference #/Heading	Question	NYSIF Response
1	13	2 - Technical Specifications	Please provide the number of unique Merchant IDs in use.	6
2	13	2 - Technical Specifications	Please provide the SAQ(s) (and number of each) required to demonstrate compliance in the latest year.	See AOC attached
3	13	2 - Technical Specifications	Please provide the number of business units accepting credit cards.	2
4	13	2 - Technical Specifications	Please provide the latest complete AOC.	See AOC attached
5	13	2 - Technical Specifications	Please provide Section 1-4 of the latest completed ROC.	See AOC attached
6	13	2 - Technical Specifications	What are the due dates for the ROC(s), AOC(s), and SAQ(s)?	Target is 12/01/2023 or 2 months from vendor selection
7	13	2 - Technical Specifications	Please describe the different acceptance channels currently in use	See AOC attached
8	13	2 - Technical Specifications	Please provide the rough number of physical locations where credit cards are accepted, processed, transmitted, or stored	See AOC attached
9	110	Mandatory Requirement Certification	Item one states that "Bidders must be a certified QSA as per the PCI Security Standards Council." Can a subcontractor fulfill this requirement?	Prime must be registered
10	13	2.2 Specifications	How many payment channels do you have (POS, E-commerce, Mobile Apps)?	See AOC attached
11	13	2.2 Specifications	How many websites process payment transactions?	0, see AOC attached
12	13	2.2 Specifications	How many departments, business units, or areas have access to cardholder data?	1, see AOC attached
13	13	2.2 Specifications	How many system components are in scope for PCI DSS compliance (servers, network devices, databases, firewalls, etc.)?	Information will be provided to selected bidder.
14	13	2.2 Specifications	Is cardholder data stored?¿How many databases and/or files store this data?	No
15	13	2.2 Specifications	How many locations process, transmit or store cardholder data (datacenters, call centers, customer service areas, etc.)? Where are these located?	2

Payment Card Industry (PCI) Compliance Testing
IFB 2023-43-INS
Amendment 1

Question #	IFB Page #	IFB Section and Sub-Section Reference #/Heading	Question	NYSIF Response
16	13	2.2 Specifications	Have your organization passed an official PCI DSS assessment previously?	Yes, see AOC attached
17	N/A	General	How many locations do you have and how many locations that accept credit cards will be included in the Assessment or ongoing support?	2
18	N/A	General	Do you have a centralized IT department that supports all locations and departments or does each location or department have their own IT Support?	Information will be provided to selected bidder
19	N/A	General	Do you have a PCI committee in place and if so what are their names and titles?	Yes, names and titles are not relevant for this IFB
20	N/A	General	What is your Merchant Level?	See AOC attached - level 4
21	N/A	General	Do you know your transaction volume?	Yes
22	N/A	General	How many merchants do you have?	6 Merchant IDs
23	N/A	General	How many SAQs do you currently fill out?	1
24	N/A	General	What SAQs are you currently filling out?	See AOC attached
25	N/A	General	Who completes the SAQs?	Selected vendor
26	N/A	General	Who do you currently submit your SAQs to?	Information will be provided to selected bidder.
27	N/A	General	How do you accept payment cards today?	See AOC attached
28	N/A	General	What systems accept payment cards?	See AOC attached
29	N/A	General	Who is your banking partner?	Information will be provided to selected bidder.
30	N/A	General	Who is your payment card processor?	Information will be provided to selected bidder.
31	N/A	General	Have you had an assessment completed before?	Yes, see AOC attached
32	N/A	General	If yes, by who? when?	Information will be provided to selected bidder.
33	N/A	General	Do you know if you require penetration testing, segmentation testing, or ASV scans?	No, see AOC attached
34	N/A	General	Would you like a PCI Portal with this contract? The vendor question is based around software used by many entities that helps with the organization of PCI as a whole. Many portals store and organize SAQs, SAQs are completed electronically, you can centralize the supporting documentation for the entity as a whole, you have the ability to request ASV scans and store the results, record hardware inventory, and various reporting features.	Out of Scope

Question #	IFB Page #	IFB Section and Sub-Section Reference #/Heading	Question	NYSIF Response
35	N/A	General	How do you satisfy your annual training requirements?	Information will be provided to selected bidder.
36	N/A	General	Onsite or Remote?	Information will be provided to selected bidder.
37	N/A	N/A	Assuming that you have undergone a PCI audit in the past, would a copy of the final contract and amount proposed by the previous year's successful vendor be available?	No
38	13	2.2	What level Merchant/Service Provider are you? Are you looking for us to complete a SAQ (if so, which one(s)) or a ROC?	See AOC attached - Level 4
39	13	2.2	Please provide an overview of your CDE technical infrastructure with a high-level idea of how many systems are in place and the types/makes of technologies involved.	Information will be provided to selected bidder.
40	13	2.2	Please provide the number of locations in scope for the audit. Also, please provide the specific locations/addresses as well along with a description of what is housed where.	Information will be provided to selected bidder.
41	13	2.2	Please provide a high-level description of the PCI cardholder data flow, what kinds of card transactions you are involved with, as well as any other information related to the nature and scope of this PCI audit.	See AOC attached
42	13	2.2 SPECIFICATIONS	When is your 2023 annual PCI DSS v3.2.1 Attestation of Compliance (AoC) due?	See AOC attached
43	13	2.2 SPECIFICATIONS	You need to complete a Report on Controls (RoC) with an AoC, but in #3 of the specifications you add "and associated SAQs". Which SAQs are needed with the RoC?	See AOC attached
44	13	2.2 SPECIFICATIONS	On #2 of the specifications, does NYSIF have the staff to perform the remediation of findings or PCI 4.0? If not, will the contractor need to assist?	NYSIF has the staff to perform remediation findings.
45	13	2.2 SPECIFICATIONS	Is NYSIF a merchant or service provider? If a merchant, which level of merchant or number of credit card transactions in the last 12 months?	See AOC attached; level 4; under 1,000 transactions per year in scope

Question #	IFB Page #	IFB Section and Sub-Section Reference #/Heading	Question	NYSIF Response
46	13	2.2 SPECIFICATIONS	How many sites are involved with the scope of the PCI engagement?	2
47	13	2.2 SPECIFICATIONS	Are the PCI controls centralized and maintained from the headquarters location or does each site maintain their own PCI controls?	Centralized
48	13	2.2 SPECIFICATIONS	Is there call recording for customers who need assistance with credits cards for dialing in to enter the credit card information? If so, if it in the cloud, outsourced, or on premise?	Information will be provided to selected bidder.
49	13	2.2 SPECIFICATIONS	Is the ecommerce application outsourced and hosted by a vendor? If developed internally, are the developers direct hire or contracted staff?	See AOC attached
50	13	2.2 SPECIFICATIONS	Is there an official cardholder data environment (CDE) onsite, in the cloud, outsource, or there is no CDE in scope for NYSIF?	See AOC attached
51	13	2.2 SPECIFICATIONS	Do you store cardholder information and numbers or is it just the token or nothing at all from the transactions?	See AOC attached
52	13	2.2 SPECIFICATIONS	How many sites have credit card readers, not the number of credit card readers per site?	None
53	13	2.2 SPECIFICATIONS	Do you have a documented set of roles and responsibilities for PCI 3.2.1?	Information will be provided to selected bidder.
54	13	2.2 SPECIFICATIONS	Will there be an NYSIF point of contact to schedule the interviews and collect the requested evidence?	Yes
55	13	2.2 SPECIFICATIONS	Do you have third-party vendors involved with your PCI scope? If so, do they submit you their annual AoC or will they need to be included in the NYSIF PCI interviews?	See AOC attached

Question #	IFB Page #	IFB Section and Sub-Section Reference #/Heading	Question	NYSIF Response
56	13	2.2 SPECIFICATIONS	Does NYSIF need the PCI Penetration Testing (External/Internal/Segmentation Test), Web Application Assessment, or Web Application Assessment with Mobile Apps to be part of this engagement? If so, then - What is the approximate number of active hosts/IPs/URLs exposed to the internet within the PCI CDE? - What is the approximate number of network-connected systems including, endpoints, servers, and infrastructure within the PCI CDE? - What is the number of CDE environments? - What is the approximate number of user input pages. - How many different user type profiles exist within the application? (standard user, client admin, site admin etc.). - Are there any publicly (internet) facing APIs? - What is the mobile application platform IOS and/or Android? - Does application use certificate pinning?	No, see AOC attached
57	13	2.2 SPECIFICATIONS	Does NYSIF need the PCI ASV vulnerability scans to be performed as part of this engagement? If so, then - What is the approximate number of active hosts/IPs/URLs needed internally for the PCI CDE and peripheral systems? - What is the approximate number of active hosts/IPs/URLs needed externally for the PCI CDE and peripheral systems?	No, see AOC attached

Question #	IFB Page #	IFB Section and Sub-Section Reference #/Heading	Question	NYSIF Response
58	13	2.4 COST/INVOICING	Does NYSIF want the PCI interview onsite at headquarters or at another location, or will a remote engagement by ok, unless there are card reader sites that need to be visited for the tampering process questions?	Interviews can be remote; no card readers.
59	7	SECTION 1 – GENERAL INFORMATION / 1.1 OVERVIEW OF THE NEW YORK STATE INSURANCE FUND	The Overview section does not include any information on how NYSIF stores, processes, or transmits cardholder data. Do you have a detailed description of your PCI environment that you can provide or can you provide a copy of the Attestation of Compliance associated with each payment stream?	See AOC attached
60	7	SECTION 1 – GENERAL INFORMATION / 1.1 OVERVIEW OF THE NEW YORK STATE INSURANCE FUND	How many years has NYSIF undergone PCI assessments?	1
61	7	SECTION 1 – GENERAL INFORMATION / 1.1 OVERVIEW OF THE NEW YORK STATE INSURANCE FUND	Have the conclusions of NYSIF's most recent PCI assessments all been "Compliant" (as opposed to "Not Compliant")?	See AOC attached
62	7	SECTION 1 – GENERAL INFORMATION / 1.1 OVERVIEW OF THE NEW YORK STATE INSURANCE FUND	Has NYSIF ever had a breach resulting in a compromise of its PCI systems and/or cardholder data?	No
63	13	SECTION 2 – TECHNICAL SPECIFICATIONS / 2.2 - SPECIFICATIONS	What is the payment stream or streams that require a Level 1 Report on Compliance (e.g. e-commerce, telephone order, mail order, card present, etc.)? For each payment stream, can you answer the following:	See AOC attached
64	13	SECTION 2 – TECHNICAL SPECIFICATIONS / 2.2 - SPECIFICATIONS	How does the NYSIF store cardholder data?	No, see AOC attached

Question #	IFB Page #	IFB Section and Sub-Section Reference #/Heading	Question	NYSIF Response
65	13	SECTION 2 – TECHNICAL SPECIFICATIONS / 2.2 - SPECIFICATIONS	How does the NYSIF process cardholder data?	See AOC attached
66	13	SECTION 2 – TECHNICAL SPECIFICATIONS / 2.2 - SPECIFICATIONS	Does the NYSIF transmit cardholder data?	See AOC attached
67	13	SECTION 2 – TECHNICAL SPECIFICATIONS / 2.2 - SPECIFICATIONS	Can you describe the types of systems used to store, process and/or transmit cardholder data (e.g. operating systems, databases, cloud environments, web applications, security systems)?	Information will be provided to selected bidder.
68	13	SECTION 2 – TECHNICAL SPECIFICATIONS / 2.2 - SPECIFICATIONS	Approximately how many systems (e.g. servers, workstations, security systems, web applications, firewalls, routers / switches) are used to support the PCI environment?	Information will be provided to selected bidder.
69	13	SECTION 2 – TECHNICAL SPECIFICATIONS / 2.2 - SPECIFICATIONS	Does NYSIF rely on segmentation to reduce the scope of its PCI compliance requirements?	See AOC attached
70	13	SECTION 2 – TECHNICAL SPECIFICATIONS / 2.2 - SPECIFICATIONS	Can you describe how the information systems used in the PCI environment are supported, by internal personnel, external vendors, and how are each involved?	Information will be provided to selected bidder.
71	13	SECTION 2 – TECHNICAL SPECIFICATIONS / 2.2 - SPECIFICATIONS	Historically when has your PCI assessment(s) began and ended?	NYSIF estimates 2 months.

Question #	IFB Page #	IFB Section and Sub-Section Reference #/Heading	Question	NYSIF Response
72	13	SECTION 2 – TECHNICAL SPECIFICATIONS / 2.2 - SPECIFICATIONS	Item 3 indicates more than one SAQ is completed for NYSIF. Can you describe each SAQ, what payment streams are assessed within each SAQ, and provide information related to each question above from 6 through 12? - How does NYSIF store / process / transmit cardholder data - Can you describe the types of systems used in the payment stream - How many systems in the payment stream - Does NYSIF rely on segmentation	See AOC attached
73	13	SECTION 2 – TECHNICAL SPECIFICATIONS / 2.2 - SPECIFICATIONS	Does NYSIF engage a vendor to perform vulnerability and penetration testing of its PCI environment(s) and when is that work performed?	Yes; details will be provided to selected bidder
74	13	SECTION 2 – TECHNICAL SPECIFICATIONS / 2.2 - SPECIFICATIONS	Can you elaborate on expectations for 2.2., number 4 - "Provide guidance associated with PCI DSS v4.0" (e.g. providing trainings/consultation to key stakeholders versus being imbedded as part of a project team)?	Gap analysis
75	13	Section 2	Who is requiring you to report PCI status? Are they requesting a RoC, SAQ, or multiple?	Payment processor
76	13	Section 2	How many payment channels do you have that intake cardholder data?	See AOC attached
77	13	Section 2	How many applications or platforms are used to take payments?	See AOC attached
78	13	Section 2	Is payment card numbers/cardholder data being stored at any time?	No
79	13	Section 2	Do you have the ability to see full payment card numbers later after payments are completed?	No
80	13	Section 2	Do your customers or employees verbally read payment card numbers over the phone? If so, are calls recorded?	See AOC attached

Question #	IFB Page #	IFB Section and Sub-Section Reference #/Heading	Question	NYSIF Response
81	13	Section 2	Do you use a VoiceOverIP platform? If so, is it managed in house or by a 3rd party?	Information will be provided to selected bidder.
82	13	Section 2	Do you type in payment card numbers into workstations (PCs or laptops)?	See AOC attached
83	13	Section 2	How many data centers do you have? Any 3rd party co-locations?	2
84	13	Section 2	Is any portion of your environment stored in the cloud? If so, which one(s)?	Information will be provided to selected bidder.
85	13	Section 2	Do you have segmentation in place in your network?	See AOC attached
86	13	Section 2	Do you rely on any third parties to take payments for you? Or do you send card numbers to 3rd parties?	See AOC attached
87	13	Section 2	What is your business model or usage for handling payment card numbers (debit/credit)?	See AOC attached
88	13	Section 2.3	What was you experience with the last vendor selected to perform PCI Assessment?	Not Relevant for this IFB
89	16	Section 3.1	When is your deadline for compliance? Are there multiple deadlines?	Target is 12/01/2023 or 2 months from vendor selection
90	17 (PDF pg. 17)	4.2 BID FORMAT	In regards to Section 4.2, the IFB states that "*Bidders must submit each of the complete Administrative, Technical, and Cost Proposals as separate electronic files on a single USB flash drive OR within the email submission* ." However, the IFB is not clear as to what content is to be included in the "Administrative" proposal. Please clarify what Bidders are to include in the separate "Administrative" Proposal.	Administrative proposal includes the Appendices, NDA and Fee Schedule
91	18-20 and 20 (PDF pgs. 18-20 and 20)	4.2 BID FORMAT and 4.27 APPENDICIES	Please confirm that all sections listed on pages 18-19 in the IFB are to go into the "Technical" Proposal with the exception of "Appendix Z Fee Schedule," which should go into the separate "Cost" Proposal. If not, please clarify.	Administrative proposal includes the Appendices, NDA and Fee Schedule. The remaining response is the technical portion of your proposal.

Question #	IFB Page #	IFB Section and Sub-Section Reference #/Heading	Question	NYSIF Response
92	7 (PDF pg. 7)	1.2 INQUIRIES/ISSUING OFFICE/DESIGNATED CONTACT	In Section 1.2 of the IFB, it states, "*All applicable amendment information must be incorporated into the firm's proposal.*" In which proposal should Bidders acknowledge addenda: Administrative, Technical, or Cost? Please clarify.	Bidders must incorporate any applicable amendments in their proposal response depending on what the amendment outlines.
93	1-10 (PDF pgs. 75-84)	Appendix E, Vendor Responsibility Questionnaire	Appendix E (Vendor Responsibility Questionnaire) does not allow Bidders to enter their NYS Vendor ID in the header of each page. Will NYSIF be reissuing a new form to all Bidders or should Bidders over right "000000000" with their NYS Vendor ID?	Vendor can enter the ID number to the right of the address on page 2 of Appendix E.
94	13 (PDF pg. 13)	2.2 Specifications	What type of PCI consulting is NYSIF looking for besides the annual audit?	As stated in the IFB
95			What merchant level does NYSIF fall under?	See AOC attached - Level 4
96			How many CDE environments do you have?	See AOC attached
97			Do you want the 5 years of audits performed onsite or remotely?	Remote preferred
98			Approx number of transactions?	Under 1,000 per year
99			How many merchant IDs are used?	6
100			Which payment software are you using?	Information will be provided to selected bidder.
101			Are CDE environments segmented?	Yes
102			If pen testing will be included in this scope, please respond to these additional questions: a. Number of CDE environments b. For each CDE: i. Please provide approximate number of active hosts/IPs/URLs exposed to the internet within the PCI CDE. ii. Please provide approximate number of network-connected systems including, endpoints, servers, and infrastructure within the PCI CDE.	Not in scope
103			What is the desired report: a. SAQ (A, A-EP, B, B-IP, C, C-VT, P2PE, or D) b. What is the number of reports required?	SAQ C at a minimum

Question #	IFB Page #	IFB Section and Sub-Section Reference #/Heading	Question	NYSIF Response
104			What elements of the ecommerce platform, if any, are hosted by NYSIF?	See AOC attached
105			Please describe the telephony technology that customer service representatives utilize to receive calls (e.g., VoIP, soft-phones, POTS, etc.). Is this infrastructure hosted by NYSIF or by a third-party?	Information will be provided to selected bidder.
106			What is the number of servers in your Cardholder Data Environment (CHD), keeping in mind that if there is no network segmentation, the entire enterprise comprises the CHD?	Information will be provided to selected bidder.
107			What is the number and types of platforms (Operating Systems) in the CHD environment (Windows, Linux, Cisco, Check Point f5, hypervisors, mainframe, VOIP, etc.)?	Information will be provided to selected bidder.
108			How many authentication mechanisms are in scope? (TACACS, RADIUS, Local, AD, etc.)	Information will be provided to selected bidder.
109			What is the number of facilities that store/transmit/process CHD (data center, call center, retail location, office facility, etc.)? a. Which sites are hosted by a PCI compliant service provider? b. Which sites are owned and managed by your organization?	2 facilities; further details will be provided to selected bidder.
110			Has penetration testing ever been performed in the environment?	Yes
111			Has a segmentation validation test been performed in the environment?	Information will be provided to selected bidder.
112			Is an accurate and complete inventory of all in-scope system components and networks maintained?	Yes
113			Are you looking for quarterly ASV network scanning?	No
114			How many physical locations accept Walk-In Card-Present payments?	Zero
115			How many locations accept Phone-Based Card-Not Present payments?	2
116			Is cardholder data stored on paper copies/receipts?	No

Question #	IFB Page #	IFB Section and Sub-Section Reference #/Heading	Question	NYSIF Response
117			Can we have a cardholder data flow diagram for all types of transactions?	Information will be provided to selected bidder.
118			Do you have any other compliance mandates (i.e., HIPAA, FISMA, SOX, GLBA, etc.)?	Out of scope
119			How many different POS systems do you use? What type and what version of POS?	Zero
120			Has a PCI DSS 4.0 readiness assessment been performed to date? If no, is that expected to be completed within the engagement hours?	No; yes it is in scope for this procurement.
121	5 (PDF pg. 63)	Exhibit C, Section 7., A. Disaster Recovery Plan	Exhibit C, Section 7 A. mentions an “Attachment A”. Would NYSIF please provide "Attachment A" for our review?	When the contract is fully executed, the IFB will be referenced as 'Attachment A' in the contract package. So any mention of Attachment A within Exhibit C, can be understood as referencing the IFB itself."
122	6 (PDF pg. 64)	Exhibit C, Section 8. Product Delivery	If awarded, or prior to award, (vendor name redacted) requests the ability to negotiate this provision, as all products will be shipped directly from the manufacturer. As a reseller, (vendor name redacted) will work with the applicable manufacturer to ensure deadlines are met to the extent possible but cannot guarantee firm delivery dates. Please advise if this would be acceptable?	All comments and limitations to Exhibit C should be included within your proposal as outlined in IFB Section 4.2.6. This will be reviewed should your firm be awarded a contract.
123	6 (PDF pg. 64)	Exhibit C, Section 10. Shipping/Receipt of Product	If awarded, or prior to award, (vendor name redacted) requests the ability to negotiate this provision for any products that might be warehoused or staged.	All comments and limitations to Exhibit C should be included within your proposal as outlined in IFB Section 4.2.6. This will be reviewed should your firm be awarded a contract.
124	7 (PDF pg. 65)	Exhibit C, Section 14. Title and Risk of Loss	If awarded, or prior to award, (vendor name redacted) requests to clarify that title and risk of loss shall be transferred to customer no later than delivery. Please advise if this would be acceptable?	All comments and limitations to Exhibit C should be included within your proposal as outlined in IFB Section 4.2.6. This will be reviewed should your firm be awarded a contract.
125	10 (PDF pg. 68)	Exhibit C, Section 24. Product Acceptance - Hardware and Software	If awarded or prior to award, (vendor name redacted) requests that if our comment above for Section 14 cannot be addressed, that Section 24 be updated to reflect that NYSIF shall have 30 days from date of delivery to accept all products (not just hardware).	All comments and limitations to Exhibit C should be included within your proposal as outlined in IFB Section 4.2.6. This will be reviewed should your firm be awarded a contract.

Payment Card Industry (PCI) Compliance Testing
IFB 2023-43-INS
Amendment 1

Question #	IFB Page #	IFB Section and Sub-Section Reference #/Heading	Question	NYSIF Response
126	12-13 (PDF pgs. 70-71)	Exhibit C, Section 35. Non-Solicitation	Would NYSIF be willing to make this section mutual, instead of one-way?	All comments and limitations to Exhibit C should be included within your proposal as outlined in IFB Section 4.2.6. This will be reviewed should your firm be awarded a contract.
127	4 (PDF pg. 114)	Mutual NDA, Section 6. Information Security Breach	Can the vendor agree to provide information no later than 24 hours after discovery of the breach. Please advise if this is acceptable?	All comments and limitations to the NDA should be included within your proposal as outlined in IFB Section 4.2.6. This will be reviewed should your firm be awarded a contract.
128	13 OF 26	PAYMENT CARD INDUSTRY (PCI) COMPLIANCE TESTING SECTION 2 TECHICAL SPECIFICATIONS 2.2 SPECIFICATIONS	What payment channels are in use, ecommerce, card present, mail order/phone order?	See AOC attached
129	13 OF 26	PAYMENT CARD INDUSTRY (PCI) COMPLIANCE TESTING SECTION 2 TECHICAL SPECIFICATIONS 2.2 SPECIFICATIONS	Do personnel have access to cardholder data? 20.How many personnel (approximate) within your organization have access to PCI data?	Yes; 10 people
130	13 OF 26	PAYMENT CARD INDUSTRY (PCI) COMPLIANCE TESTING SECTION 2 TECHICAL SPECIFICATIONS 2.2 SPECIFICATIONS	How many physical locations transmit, process or store cardholder data?	2
131	13 OF 26	PAYMENT CARD INDUSTRY (PCI) COMPLIANCE TESTING SECTION 2 TECHICAL SPECIFICATIONS 2.2 SPECIFICATIONS	Network - Include number and types of zones/VLANs that are expected to be in scope for PCI.	Information will be provided to selected bidder.
132	13 OF 26	PAYMENT CARD INDUSTRY (PCI) COMPLIANCE TESTING SECTION 2 TECHICAL SPECIFICATIONS 2.2 SPECIFICATIONS	How many firewalls are in scope?	Information will be provided to selected bidder.

Question #	IFB Page #	IFB Section and Sub-Section Reference #/Heading	Question	NYSIF Response
133	13 OF 26	PAYMENT CARD INDUSTRY (PCI) COMPLIANCE TESTING SECTION 2 TECHICAL SPECIFICATIONS 2.2 SPECIFICATIONS	Is wireless used in the cardholder data environment?	Information will be provided to selected bidder.
134	13 OF 26	PAYMENT CARD INDUSTRY (PCI) COMPLIANCE TESTING SECTION 2 TECHICAL SPECIFICATIONS 2.2 SPECIFICATIONS	Database – Include type and number of database systems that store CHD or payment information tokens/auth codes.	Zero
135	13 OF 26	PAYMENT CARD INDUSTRY (PCI) COMPLIANCE TESTING SECTION 2 TECHICAL SPECIFICATIONS 2.2 SPECIFICATIONS	Applications – How many internally developed payment applications and, separately, third-party payment applications.	One 3rd party
136	13 OF 26	PAYMENT CARD INDUSTRY (PCI) COMPLIANCE TESTING SECTION 2 TECHICAL SPECIFICATIONS 2.2 SPECIFICATIONS	Number of Windows servers in-scope.	Information will be provided to selected bidder.
137	13 OF 26	PAYMENT CARD INDUSTRY (PCI) COMPLIANCE TESTING SECTION 2 TECHICAL SPECIFICATIONS 2.2 SPECIFICATIONS	Number of Linux/Unix servers in-scope.	Information will be provided to selected bidder.
138	13 OF 26	PAYMENT CARD INDUSTRY (PCI) COMPLIANCE TESTING SECTION 2 TECHICAL SPECIFICATIONS 2.2 SPECIFICATIONS	Number of AS400, Midframe/Mainframe in scope.	Zero
139	13 OF 26	PAYMENT CARD INDUSTRY (PCI) COMPLIANCE TESTING SECTION 2 TECHICAL SPECIFICATIONS 2.2 SPECIFICATIONS	Number of workstations in-scope	20

Question #	IFB Page #	IFB Section and Sub-Section Reference #/Heading	Question	NYSIF Response
140	13 OF 26	PAYMENT CARD INDUSTRY (PCI) COMPLIANCE TESTING SECTION 2 TECHICAL SPECIFICATIONS 2.2 SPECIFICATIONS	Are call centers in-scope?	See AOC attached
141	13 OF 26	PAYMENT CARD INDUSTRY (PCI) COMPLIANCE TESTING SECTION 2 TECHICAL SPECIFICATIONS 2.2 SPECIFICATIONS	2.2 says 'Annual Completion of the Attestation of Compliance and associated SAQs.' as one of the deliverables. Can you elaborate on if there are subsidiaries that would need separate SAQs? If so, please list the entity and the related SAQ that would be needed.	See AOC attached
142	13 OF 26	PAYMENT CARD INDUSTRY (PCI) COMPLIANCE TESTING SECTION 2 TECHICAL SPECIFICATIONS 2.2 SPECIFICATIONS	Approximately how many annual credit card transactions are processed through your system?	Merchant level 4
143	13 OF 26	PAYMENT CARD INDUSTRY (PCI) COMPLIANCE TESTING SECTION 2 TECHICAL SPECIFICATIONS 2.2 SPECIFICATIONS	Internal and External Penetration testing and vulnerability scans are required as part of PCI compliance. Do you require these services?	No
144	13 OF 26	PAYMENT CARD INDUSTRY (PCI) COMPLIANCE TESTING SECTION 2 TECHICAL SPECIFICATIONS 2.2 SPECIFICATIONS	If you have previously undergone a PCI DSS Assessment, have you complied with the requirements of the quarterly passing ASV scans and the internal and external penetration tests where required?	Yes
145	13 OF 26	PAYMENT CARD INDUSTRY (PCI) COMPLIANCE TESTING SECTION 2 TECHICAL SPECIFICATIONS 2.2 SPECIFICATIONS	Are there any commitments to your clients / stakeholders to provide the report by a particular date? a.If so what is the Date of your commitment?	Target is 12/01/2023 or 2 months from vendor selection.
146	13 OF 26	PAYMENT CARD INDUSTRY (PCI) COMPLIANCE TESTING SECTION 2 TECHICAL SPECIFICATIONS 2.2 SPECIFICATIONS	Are there any parts of your organizations processes or controls for storing, processing, and transmitting Cardholder Data that are outsourced to a third-party vendor (also referred to as a sub-service organization) that should be included within the scope of this review?	See AOC attached

Question #	IFB Page #	IFB Section and Sub-Section Reference #/Heading	Question	NYSIF Response
147	13 OF 26	PAYMENT CARD INDUSTRY (PCI) COMPLIANCE TESTING SECTION 2 TECHICAL SPECIFICATIONS 2.2 SPECIFICATIONS	Are there any anticipated significant changes to the applications or IT systems including new implementation or significant upgrades to applications / IT systems?	Information will be provided to selected bidder.
148	13 OF 26	PAYMENT CARD INDUSTRY (PCI) COMPLIANCE TESTING SECTION 2 TECHICAL SPECIFICATIONS 2.2 SPECIFICATIONS	Does your organization perform programming and development efforts of the production applications? a.If yes, please provide a high-level overview of tools used for software development / maintenance and any supporting systems to track the SDLC / Change Controls process.	Information will be provided to selected bidder.
149	13	IFB #2023-43-INS	Number of ASV Scans for External Facing IP Addresses in Cardholder Data Environment	See AOC attached
150	13	IFB #2023-43-INS	Number of IP Addresses for Penetration Testing external Facing in Cardholder Data Environment	Information will be provided to selected bidder.
151	13	IFB #2023-43-INS	Number of IP Addresses for Penetration Testing internal Facing in Cardholder Data Environment	Information will be provided to selected bidder.
152	13	IFB #2023-43-INS	Number of IP Addresses for Vulnerability Assessments internal Facing in Cardholder Data Environment	Information will be provided to selected bidder.
153	13	IFB #2023-43-INS	Number of IP Addresses for Vulnerability Assessments external Facing ex Cardholder Data Environment	Information will be provided to selected bidder.
154	13	IFB #2023-43-INS	Number of Security Configurations (if applicable to this attestation)	Information will be provided to selected bidder.
155	13	IFB #2023-43-INS	How many Assets are in your Cardholder Data Environment to be tested	Information will be provided to selected bidder.
156	13	IFB #2023-43-INS	Number if Firewall Rule Sets to Review to be tested	Information will be provided to selected bidder.
157	13	IFB #2023-43-INS	Number of VLANS tested to be tested	Information will be provided to selected bidder.
158	13	IFB #2023-43-INS	Number of Wireless access Points to be tested	Information will be provided to selected bidder.
159	13	IFB #2023-43-INS	Number of Applications in Cardholder Data Environment to be tested	Information will be provided to selected bidder.
160	13	IFB #2023-43-INS	Number of APIs touching your Cardholder Data Environment to be tested	Information will be provided to selected bidder.
161	13	IFB #2023-43-INS	How many Servers both Web and OS are in your Cardholder Data Environment to be tested	Information will be provided to selected bidder.

Question #	IFB Page #	IFB Section and Sub-Section Reference #/Heading	Question	NYSIF Response
162	13	IFB #2023-43-INS	How many Network devices are inside of your Card Holder Environment	Information will be provided to selected bidder.
163	13	IFB #2023-43-INS	Are your these services hosted or on Prem if Hosted please list where they are hosted.	Information will be provided to selected bidder.
164	110	Mandatory Requirement Certification	Item one states that "Bidders must be a certified QSA as per the PCI Security Standards Council." Can a subcontractor partner fulfill this requirement?	Prime must be registered.
165	13	2.2 Specifications	This item appears to be in conflict with Appendix Z which includes a Gap Analysis & Assessment in addition to the actual audit. Are you seeking a gap analysis prior to the actual audit to determine where weaknesses may exist before you undertake the audit?	The Gap analysis is for transition to PCI 4.0. The audit is for the current PCI v3.8.
166	13	2.2 Specifications	Is the portion of the network where PCI data resides segmented from the remainder of the network?	Information will be provided to selected bidder.
167	13	2.2 Specifications	How large is the network that will be examined for PCI requirements?	Information will be provided to selected bidder.
168	13	2.2 Specifications	What is your due date for submitting the ROC (Report on Compliance)?	Target is 12/01/2023 or 2 months from vendor selection
169	13	2.2 SPECIFICATIONS	Item 1 indicates Report on Compliance; however, the last paragraph suggests the vendor follow guidance for SAQ. Please clarify which PCI Level NYSIF is designated.	NYSIF is Level 4
170	13	2.2 SPECIFICATIONS	Item 1 indicates " (PCI DSS v4 when it takes effect in 2024)". The effective date for v4 is March 31, 2025. Please clarify if NSIF wishes to adopt PCI DSS v4.0 when reporting in 2024.	NYSIF wishes to comply on or before the effective date.
171	13	2.2 SPECIFICATIONS	Item 3 indicates completion of SAQs. Please clarify which SAQ form is being used.	See AOC attached
172	N/A		Does NYSIF store cardholder data?	No
173	N/A		What payment channels does NYSIF support? Examples include e-commerce, card-present using a terminal, unattended kiosks, mobile application, etc.	See AOC attached

Question #	IFB Page #	IFB Section and Sub-Section Reference #/Heading	Question	NYSIF Response
174	N/A		Has NYSIF been assessed before?	Yes
175	N/A		Does NYSIF have a call center which accepts cardholder data by phone or mail order?	Yes
176	N/A		If using e-commerce, is this direct post, iFrame, redirect, or other?	Not in scope
177	N/A		Is the environment on premise, hosted, or both?	Information will be provided to selected bidder.
178	N/A		How many systems are in scope for this assessment?	Information will be provided to selected bidder.
179	N/A		How many types of systems are in scope for this assessment?	Information will be provided to selected bidder.
180	N/A		Is there a desired start or end date for this assessment?	Target for the report is 12/01/2023 or 2 months from vendor selection.