NEW YORK STATE OF OPPORTUNITY. Department of Civil Service

NYSIF Vendor Security Survey - RFP entitled: "Pharmacy Benefit Services for The Empire Plan, Student Employee Health Plan, and NYS Insurance Fund Workers' Compensation Prescription Drug Programs"

REQUIREMENTS

The Vendor Security Survey & Vendor Profile (Appendix B-3) is to be submitted as part of the bid or proposal package. Bidders are required to answer all of the questions in order to be considered for an award of a contract with the New York State Insurance Fund (NYSIF).

The completed Vendor Security Survey section of Appendix B-3 will be reviewed and evaluated by NYSIF personnel on a pass/fail basis. The minimum required implementation levels are included in the surveyand defined below. Bidders who do not meet the minimum required implementation levels will be disqualified.

INSTRUCTIONS FOR COMPLETION

For purposes of this Appendix B-3 and notwithstanding any other definition in the Agreement to whichthis Appendix B-3 is attached and incorporated, the following terms have special meanings:

"NYSIF's Information or Data" shall have the same meaning as the term "Nonpublic Information," as defined in the New York State Department of Financial Services Cybersecurity Regulation at 23 N.Y.C.R.R. § 500.1, and shall include NYSIF information for which disclosure is prohibited or restricted pursuant to Workers' Compensation Law §§ 98 or 110-a. This term is used in Questions A and B.

Personal Information means "record" information, including "Individually Identifiable Information," as the terms are defined in the Worker's Compensation Law § 110-a, non-public "Individually Identifiable Health Information," as such term is defined in 42 U.S.C. § 1320d, and individual financial information that would be confidential pursuant to 12 U.S.C. § 3403 if held by a financial institution.

Within the ***"RESPONSE"*** column all questions must be answered by selecting the appropriate answer from the drop-down list, providing an explanation of the controls, and providing substantiating document(s). The drop-down list is defined as follows:

1. **Fully** (Implemented) = The control is in place, functioning effectively, and is optimized.
2. **Partially** (Implemented) = The control is in place, effectiveness may not be rated, and the control is not optimized.
3. **Non-Existent** = The control is not in place.

*Note: Section 1, Data Privacy, Questions A, B, C and D have a different drop down of 'Yes' or 'No', with a request to further explain in the "Explanation of Controls" Section.

Within the ***"EXPLANATION OF CONTROLS"*** column, comments must be provided to support a bidder's' selected ***"RESPONSE".*** Comments must clarify the controls implemented, describe mitigating factors, such as alternative controls or exposure limits, and specify the date when the control will be operational.

Within the ***"SUBSTANTIATING DOCUMENT(S)"*** column, supporting documentation is optional. Documentation should support a bidder's response, such as written policy, audits, screenshots, etc.

All questions related to this Vendor Security Survey & Vendor Profile must be submitted in writing to contracts@nysif.com by the date and time indicated in the solicitation calendar, citing the question and bid number.

VENDOR COMPANY INFORMATION	VENDOR RESOURCE COMPLETING QUESTIONNAIRE
NAME	
ADDRESS	
CITY/STATE/ZIP	

General Instructions: The following questions are divided by Critical Security Control topic. Details entered within the "Explanation of Controls" should clarify and explain the response to the data request as well as explain exposure limits that may apply. Provide references to any supporting documentation included along with the survey within "Substantiating Document(s)". For example, "See attached documentation - <filename1.pdf>, <filename2.docx>."

Bidder Affirmation: Bidder affirms understanding and agreeing to the mandatory technical requirements described in the Bid Documents and inquired about in this Appendix B-3, and provides its responses to the inquiries in this Appendix B-3 and signature of its authorized representative who completed this Appendix B-3 certifying that Contractor meets such mandatory technical requirements. Bidder further affirms and agrees that if Bidder is awarded the contractfor which this Appendix B-3 is submitted that the responses to this Appendix B-3, as well as any and all responses to Data Requests from NYSIF for supplemental information completed and submitted by Bidder, will be incorporated in andattached to the Agreement between NYSIF and Bidder.

INSTRUCTIONS FOR "EXPLANATION OF CONTROLS"	INSTRUCTIONS FOR "SUBSTANTIATING DOCUMENT(S)"
Within the "EXPLANATION OF CONTROLS" column, comments MUST be provided to support a bidder's' selected "RESPONSE". Comments must clarify the controls implemented, describe mitigating factors, such as alternative controls or exposure limits, and specify the date when the control will be operational. Appendix B-3 WILL NOT be accepted if "EXPLANATION OF CONTROLS" is left blank for ANY of the questions below.The MINIMUM Required Level for Controls 1-20 is PARTIALLY.	Within the "SUBSTANTIATING DOCUMENT(S)" column, supporting documentation is not required if the "EXPLANATION OF CONTROLS" provides sufficient detail.

	DATA PRIVACY	RESPONSE	EXPLANATION OF CONTROLS	SUBSTANTIATING
A	Bidder asserts NYSIF's Information or Data is **NOT** transmitted outside of or accessed from outside of the United States. Please explain how this is accomplished in the Explanation of Controls box.			
B	Do you use one or more cloud service providers to store NYSIF's Information or Data? Please describe how you secure it in the Explanation of Controls box.			
C	Do you use Multi-Factor Authentication (MFA) for users to connect to your internal network? Please describe the MFA used (FIDO/WebAuthn, Authenticator App, etc.)			
D	Do you have a Cybersecurity Vendor Risk Management program or process in place for your third party vendors? Please describe in the Explanation of Controls box.			

	INVENTORY OF AUTHORIZED AND UNAUTHORIZED DEVICES	RESPONSE	EXPLANATION OF CONTROLS	SUBSTANTIATING DOCUMENT(S)
1	Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.			
	INVENTORY OF AUTHORIZED AND UNAUTHORIZED SOFTWARE	**RESPONSE**	**EXPLANATION OF CONTROLS**	**SUBSTANTIATING DOCUMENT(S)**
2	Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.			
	SECURE CONFIGURATIONS FOR HARDWARE AND SOFTWARE	**RESPONSE**	**EXPLANATION OF CONTROLS**	**SUBSTANTIATING DOCUMENT(S)**
3	Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings. **Additional Information for Vendors:** Since many systems don't come out-of-the-box secured, the purpose of this control is to maintain documented, standard security configuration standards for all authorized operating systems and software. Your organization should among others 1) create security baselines for every system using established resource; 2) use a rigorous configuration management and change control process; 3) use a compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.			
	CONTINUOUS VULNERABILITY ASSESSMENT AND REMEDIATION	**RESPONSE**	**EXPLANATION OF CONTROLS**	**SUBSTANTIATING DOCUMENT(S)**
4	Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers. **Additional Information for Vendors:** Organizations that do not scan for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their computer systems compromised. To achieve compliance with this control, you will need to show your organization has 1) implemented automated vulnerability scanning tools (not to be confused with Anti-Virus scanning tools or a Penetration test) against all systems on a weekly or more frequent basis, 2) deployed automated patch management & software update tools 3) routinely monitor event logs.			

	CONTROLLED USE OF ADMINISTRATIVE PRIVILEGES	RESPONSE	EXPLANATION OF CONTROLS	SUBSTANTIATING DOCUMENT(S)
5	The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications. **Additional Information for Vendors:** The misuse of administrative privileges is a primary method for attackers to spread inside a target enterprise. Controls should be implemented by job role and follow the principles of least privilege to accomplish the job, change default passwords, use dedicated accounts with multi-factor authentication for elevated access and activities, logging and monitoring such access etc.			
	MAINTENANCE, MONITORING, AND ANALYSIS OF AUDIT LOGS	**RESPONSE**	**EXPLANATION OF CONTROLS**	**SUBSTANTIATING DOCUMENT(S)**
6	Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.			
	EMAIL AND WEB BROWSER PROTECTIONS	**RESPONSE**	**EXPLANATION OF CONTROLS**	**SUBSTANTIATING DOCUMENT(S)**
7	Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems. **Additional Information for Vendors:** Web browsers and email are easy entry points for attackers. Please: 1) demonstrate that only fully supported web browsers and email clients are allowed to execute in the organization; 2) implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the Domain Keys Identified Mail (DKIM) standards for email security.			
	MALWARE DEFENSES	**RESPONSE**	**EXPLANATION OF CONTROLS**	**SUBSTANTIATING DOCUMENT(S)**
8	Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.			

	LIMITATION AND CONTROL OF NETWORK PORTS	RESPONSE	EXPLANATION OF CONTROLS	SUBSTANTIATING DOCUMENT(S)
9	Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.			
	DATA RECOVERY CAPABILITY	**RESPONSE**	**EXPLANATION OF CONTROLS**	**SUBSTANTIATING DOCUMENT(S)**
10	The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it. **Additional Information for Vendors:** When systems get compromised, it can be extremely difficult for organizations without a trustworthy data recovery capability to remove all aspects of the attacker's presence on the machine. Please show 1) that all system data is automatically backed up on regular basis; 2) that each of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.			
	SECURE CONFIGURATIONS FOR NETWORK DEVICES	**RESPONSE**	**EXPLANATION OF CONTROLS**	**SUBSTANTIATING DOCUMENT(S)**
11	Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings. **Additional Information for Vendors:** By default network infrastructure devices are not secured adequately. They are generally delivered with default configurations, open services and ports, default accounts or passwords, support for vulnerable protocols. Detail how you: 1) Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered; 2) Manage all network devices using multi-factor authentication and encrypted sessions.			
	BOUNDARY DEFENSE	**RESPONSE**	**EXPLANATION OF CONTROLS**	**SUBSTANTIATING DOCUMENT(S)**
12	Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data. **Additional Information for Vendors:** Traffic through network borders should be controlled and monitored for attacks and evidence of compromised machines. Boundary defenses should be multi-layered, relying on firewalls, proxies, Demilitarized Zone (DMZ) perimeter networks, and network-based intrusion detection and prevention systems. It is critical to filter both inbound and outbound traffic and require all remote login access to the organization's network to encrypt data and use multi-factor authentication.			

	DATA PROTECTION	RESPONSE	EXPLANATION OF CONTROLS	SUBSTANTIATING DOCUMENT(S)
13	The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information, including Personal Information received from NYSIF. **Additional Information for Vendors:** Ensuring that data is protected and not compromised can be achieved through data encryption, integrity protection and data loss prevention. Encrypt hard drives and if there is no business need, disable removable media such as USB, CD, DVDs etc... If removable media is required, all data stored on such devices must be encrypted while at rest.			
	CONTROLLED ACCESS BASED ON THE NEED TO KNOW	**RESPONSE**	**EXPLANATION OF CONTROLS**	**SUBSTANTIATING DOCUMENT(S)**
14	The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.			
	WIRELESS ACCESS CONTROL	**RESPONSE**	**EXPLANATION OF CONTROLS**	**SUBSTANTIATING DOCUMENT(S)**
15	The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.			
	ACCOUNT MONITORING AND CONTROL	**RESPONSE**	**EXPLANATION OF CONTROLS**	**SUBSTANTIATING DOCUMENT(S)**
16	Actively manage the life cycle of system and application accounts -their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.			

	SECURITY SKILLS ASSESSMENT AND TRAINING	RESPONSE	EXPLANATION OF CONTROLS	SUBSTANTIATING DOCUMENT(S)
17	For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.			
	APPLICATION SOFTWARE SECURITY	**RESPONSE**	**EXPLANATION OF CONTROLS**	**SUBSTANTIATING DOCUMENT(S)**
18	Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses. **Additional Information for Vendors:** Please include information on controls around your acquired or purchased software also (including commercial off the shelf software, for example, Microsoft Office, Adobe etc...) such as using supported or latest versions, installing patches and applying security recommendations.			
	INCIDENT RESPONSE AND MANAGEMENT	**RESPONSE**	**EXPLANATION OF CONTROLS**	**SUBSTANTIATING DOCUMENT(S)**
19	Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems. **Additional Information for Vendors:** Without an incident response plan, an organization may not discover an attack in the first place, or, if the attack is detected, the organization may not follow good procedures to contain damage, eradicate the attacker's presence, and recover in a secure fashion. An effective incident response plan is a written document that defines roles of personnel as well as phases of incident handling/management. It also assembles and maintains information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors etc. Provide details about your organization's Incident Response Plan.			

	PENETRATION TESTS	RESPONSE	EXPLANATION OF CONTROLS	SUBSTANTIATING DOCUMENT(S)
20	Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker. **NOTE: An annual Penetration Test is a requirement for doing business with NYSIF. (A Statement of Work may be used to continue through the contract execution process.) Upon award Firm(s) will be required to provide Penetration Test documentation of test performed within the last 12-months. No work will be provided under the contract until this requirement has been satisfied.** **Additional Information for Vendors:** 1. What is a Penetration Test – A penetration test is an authorized security attack where certified skilled cyber security experts attempt to find and exploit vulnerabilities in your organization's computer systems or network. The test identifies any loopholes or weaknesses you may have. This should not be confused with vulnerability assessments which may be part of a penetration test but not a substitute for it. 2. The Importance of a Penetration Test - The test is a simulated attack to identify any weaknesses in a system's defenses that attackers could take advantage of. This is so any information, especially sensitive information is not stolen by a hacker. Penetration testing leverages many of the previous controls and provides feedback to help remediate vulnerabilities discovered during the test. 3. Why NYSIF requires the test - NYSIF requires a penetration test as it helps vendors uncover any hidden vulnerabilities which help identify and validate any security loopholes in their systems. 4. What is acceptable Penetration Test Documentation VS. Not acceptable - A penetration test is done by a certified skilled professional. Documentation should provide evidence of a completed penetration test such as: A report with findings and remediations, or an Executive Summary, or an Attestation letter from the testing company. The primary components of a Penetration Test are: a) Network Testing. b) Cloud, Web and Mobile Application Testing (Where Applicable). c) Vulnerability Scanning. d) Exploitation. e) Remediation Plan. 5. Additional information: a) The length of the penetration testing engagement depends on the type of testing and can take an average of 1 - 4 weeks not including the planning stages which could extend out to months depending on the activities the pen tester needs to perform. b) Getting a comprehensive risk picture of your company gives you an opportunity to map the identified vulnerabilities and exploits and give a summary of those risks that would have any threats materialize. c) Effectively finding and fixing any security issues should include collaboration and communication with product, security, and development teams to leverage the vulnerabilities found on the external assets.			

	VENDOR PROFILE	
	Instructions: *Please answer the questions making entries in the Response area.*	
	VENDOR SERVICE STATUS	**RESPONSE**
1	Is your organization currently providing services to NY State Insurance Fund (NYSIF), either actively or on an intermittent (ad-hoc) basis? Is your organization currently providing services to NY State Insurance Fund (NYSIF), either actively or on an intermittent (ad-hoc) basis? Note: If no longer providing services in any capacity, please provide details of service termination, dates, etc. for review and consideration.	
	SERVICE OVERVIEW	**RESPONSE**
2	Is there an executed contract between NYSIF and your organization?	
3	What is the current business relationship? (I.e. What services does your organization currently provide to NYSIF? (*Please be detailed*)	
4	Will the business relationship between NYSIF and your organization change within the next year? If so, please describe the changes.	
5	From what physical location(s) does your organization provide services to NYSIF? (Please include all locations providing services.)	
	DATA EXCHANGE	**RESPONSE**
6	Does your organization receive data from NYSIF?	
6-a	If yes, by what means is NYSIF data exchanged and in what direction; from NYSIF to your organization or both directions?	
7	Are any of the following types of data transmitted, stored, and/or processed by your organization during the course of providing services to NYSIF?	
7-a	Protected Health Information ("PHI") or Individually Identifiable Health Information, as 42 U.S.C. § 1320d?	
7-b	Payment Card Information ("PCI")?	
7-c	Individually Identifiable Information as defined in Worker's Compensation Law § 110-a ?	
7-d	Social Security Number ("SSN")	
7-e	Financial information, or information that could be covered under SOX?	
7-f	Other type of personally identifiable information, not listed above?	
8	On average, what is the volume of NYSIF data transmitted, processed, received, etc. per month by your organization?	
9	On average, what is the volume of NYSIF data stored by your organization?	
10	In the past 12 months has your organization, or any of your sub-contractors, experienced a material breach or unauthorized disclosure of any data? If yes, please describe situation, data exposed and timing in detail.	

Signature of affirming authorized representative of Bidder

Bidder's Name: _____

Authorized Representative Signature: _____

Printed or Typed Name: _____

Title of Signatory: _____

Date: _____