

## ATTACHMENT 17



**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 (Attachment 17) 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).

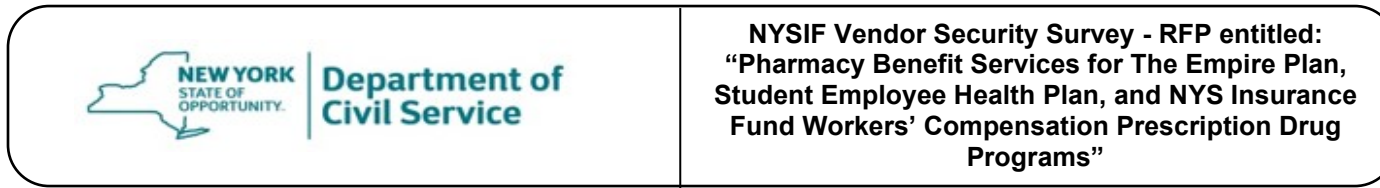
The completed Vendor Security Survey will be reviewed and evaluated by NYSIF personnel on a pass/fail basis. The minimum required implementation levels are included in the survey and defined below. Bidders who do not meet the minimum required implementation levels will be disqualified.

### **SECTION 1 INSTRUCTIONS FOR COMPLETION**

Within the "**RESPONSE**" column all questions must be answered by selecting the appropriate answer from the drop-down list and 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.

## ATTACHMENT 17




\*Note: Section 1, Data Privacy, Question B & C 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.

**SECTION 2 ALL QUESTIONS RELATED TO THIS VENDOR SECURITY SURVEY MUST BE SUBMITTED IN WRITING TO [CONTRACTS@NYSIF.COM](mailto:CONTRACTS@NYSIF.COM) BY THE DATE AND TIME INDICATED IN THE SOLICITATION CALENDAR, CITING THE PARTICULAR QUESTION AND BID NUMBER.**

# ATTACHMENT 17




**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”**


VENDOR SECURITY SURVEY				
VENDOR COMPANY INFORMATION		VENDOR RESOURCE COMPLETING QUESTIONNAIRE		
NAME		ASSIGNEE NAME		
WEBSITE		ROLE OR TITLE		
ADDRESS		PHONE + EXT		
CITY/STATE/ZIP		EMAIL ADDRESS		
INSTRUCTIONS FOR "EXPLANATION OF CONTROLS"		INSTRUCTIONS FOR "SUBSTANTIATING DOCUMENT(S)"		
Within the "EXPLANATION OF CONTROLS" column, comments <b>MUST</b> 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 T <b>WILL NOT</b> be accepted if "EXPLANATION OF CONTROLS" is left blank for ANY of the questions below.		Within the "SUBSTANTIATING DOCUMENT(S)" column, supporting documentation is not required if the "EXPLANATION OF CONTROLS" provides sufficient detail.  Documentation should support a bidder's response, such as written policy, audits, screenshots, etc.		
	DATA PRIVACY	RESPONSE	EXPLANATION OF CONTROLS	SUBSTANTIATING DOCUMENT(S)
A	Bidder asserts NYSIF's confidential/sensitive 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.	PLEASE RESPOND (Using Dropdown)		
B	Do you use one or more cloud service providers to store NYSIF's data? Describe how you secure it in the Explanation of Controls box.	PLEASE RESPOND (Using Dropdown)		
C	Do you have a Cybersecurity Vendor Risk Management program or process in place for your third party vendors? Describe in the Explanation of Controls box.	PLEASE RESPOND (Using Dropdown)		
1	<b>INVENTORY OF AUTHORIZED AND UNAUTHORIZED DEVICES</b>	RESPONSE	EXPLANATION OF CONTROLS	SUBSTANTIATING DOCUMENT(S)
	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.	PLEASE RESPOND (Using Dropdown)		
	<b>MINIMUM REQUIRED LEVEL = PARTIALLY</b>			
2	<b>INVENTORY OF AUTHORIZED AND UNAUTHORIZED SOFTWARE</b>	RESPONSE	EXPLANATION OF CONTROLS	SUBSTANTIATING DOCUMENT(S)
	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	PLEASE RESPOND (Using Dropdown)		
	<b>MINIMUM REQUIRED LEVEL = PARTIALLY</b>			
3	<b>SECURE CONFIGURATIONS FOR HARDWARE AND SOFTWARE</b>	RESPONSE	EXPLANATION OF CONTROLS	SUBSTANTIATING DOCUMENT(S)

# ATTACHMENT 17

 <div style="display: inline-block; vertical-align: middle; margin-left: 10px;"> <p><b>Department of Civil Service</b></p> </div>	<p><b>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”</b></p>
--	---


	<p>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.</p> <p><b>Additional Information for Vendors:</b> 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.</p>	<p>PLEASE RESPOND (Using Dropdown)</p>		
<b>MINIMUM REQUIRED LEVEL = PARTIALLY</b>				
<b>4</b>	<b>CONTINUOUS VULNERABILITY ASSESSMENT AND REMEDIATION</b>	<b>RESPONSE</b>	<b>EXPLANATION OF CONTROLS</b>	<b>SUBSTANTIATING DOCUMENT(S)</b>
	<p>Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.</p> <p><b>Additional Information for Vendors:</b> 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 &amp; software update tools 3) routinely monitor event logs.</p>	<p>PLEASE RESPOND (Using Dropdown)</p>		
<b>MINIMUM REQUIRED LEVEL = PARTIALLY</b>				
<b>5</b>	<b>CONTROLLED USE OF ADMINISTRATIVE PRIVILEGES</b>	<b>RESPONSE</b>	<b>EXPLANATION OF CONTROLS</b>	<b>SUBSTANTIATING DOCUMENT(S)</b>
	<p>The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.</p> <p><b>Additional Information for Vendors:</b> 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.</p>	<p>PLEASE RESPOND (Using Dropdown)</p>		
<b>MINIMUM REQUIRED LEVEL = PARTIALLY</b>				
<b>6</b>	<b>MAINTENANCE, MONITORING, AND ANALYSIS OF AUDIT LOGS</b>	<b>RESPONSE</b>	<b>EXPLANATION OF CONTROLS</b>	<b>SUBSTANTIATING DOCUMENT(S)</b>
	<p>Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.</p>	<p>PLEASE RESPOND (Using Dropdown)</p>		
<b>MINIMUM REQUIRED LEVEL = PARTIALLY</b>				
<b>7</b>	<b>EMAIL AND WEB BROWSER PROTECTIONS</b>	<b>RESPONSE</b>	<b>EXPLANATION OF CONTROLS</b>	<b>SUBSTANTIATING DOCUMENT(S)</b>

# ATTACHMENT 17

 <div style="display: inline-block; vertical-align: middle; margin-left: 20px;"> <p><b>Department of Civil Service</b></p> </div>	<p><b>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”</b></p>
--	---


	<p>Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.</p> <p><b>Additional Information for Vendors:</b> 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.</p>	<p>PLEASE RESPOND (Using Dropdown)</p>		
<b>MINIMUM REQUIRED LEVEL = PARTIALLY</b>				
<b>8</b>	<b>MALWARE DEFENSES</b>	<b>RESPONSE</b>	<b>EXPLANATION OF CONTROLS</b>	<b>SUBSTANTIATING DOCUMENT(S)</b>
	<p>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.</p>	<p>PLEASE RESPOND (Using Dropdown)</p>		
<b>MINIMUM REQUIRED LEVEL = PARTIALLY</b>				
<b>9</b>	<b>LIMITATION AND CONTROL OF NETWORK PORTS</b>	<b>RESPONSE</b>	<b>EXPLANATION OF CONTROLS</b>	<b>SUBSTANTIATING DOCUMENT(S)</b>
	<p>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.</p>	<p>PLEASE RESPOND (Using Dropdown)</p>		
<b>MINIMUM REQUIRED LEVEL = PARTIALLY</b>				

# ATTACHMENT 17

 <div style="display: inline-block; vertical-align: middle; margin-left: 10px;"> <p><b>Department of Civil Service</b></p> </div>	<p><b>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”</b></p>
--	---

10	DATA RECOVERY CAPABILITY	RESPONSE	EXPLANATION OF CONTROLS	SUBSTANTIATING DOCUMENT(S)
	<p>The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.</p> <p><b>Additional Information for Vendors:</b> 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.</p>	PLEASE RESPOND (Using Dropdown)		
	<b>MINIMUM REQUIRED LEVEL = PARTIALLY</b>			
11	SECURE CONFIGURATIONS FOR NETWORK DEVICES	RESPONSE	EXPLANATION OF CONTROLS	SUBSTANTIATING DOCUMENT(S)
	<p>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.</p> <p><b>Additional Information for Vendors:</b> 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.</p>	PLEASE RESPOND (Using Dropdown)		
	<b>MINIMUM REQUIRED LEVEL = PARTIALLY</b>			
12	BOUNDARY DEFENSE	RESPONSE	EXPLANATION OF CONTROLS	SUBSTANTIATING DOCUMENT(S)
	<p>Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.</p> <p><b>Additional Information for Vendors:</b> 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.</p>	PLEASE RESPOND (Using Dropdown)		
	<b>MINIMUM REQUIRED LEVEL = PARTIALLY</b>			
13	DATA PROTECTION	RESPONSE	EXPLANATION OF CONTROLS	SUBSTANTIATING DOCUMENT(S)
	<p>The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.</p> <p><b>Additional Information for Vendors:</b> 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.</p>	PLEASE RESPOND (Using Dropdown)		
	<b>MINIMUM REQUIRED LEVEL = PARTIALLY</b>			
14	CONTROLLED ACCESS BASED ON THE NEED TO KNOW	RESPONSE	EXPLANATION OF CONTROLS	SUBSTANTIATING DOCUMENT(S)

# ATTACHMENT 17



**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”**

	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.	PLEASE RESPOND (Using Dropdown)		
	<b>MINIMUM REQUIRED LEVEL = PARTIALLY</b>			
15	<b>WIRELESS ACCESS CONTROL</b>	RESPONSE	EXPLANATION OF CONTROLS	SUBSTANTIATING DOCUMENT(S)
	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.	PLEASE RESPOND (Using Dropdown)		
	<b>MINIMUM REQUIRED LEVEL = PARTIALLY</b>			
16	<b>ACCOUNT MONITORING AND CONTROL</b>	RESPONSE	EXPLANATION OF CONTROLS	SUBSTANTIATING DOCUMENT(S)
	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.	PLEASE RESPOND (Using Dropdown)		
	<b>MINIMUM REQUIRED LEVEL = PARTIALLY</b>			
17	<b>SECURITY SKILLS ASSESSMENT AND TRAINING</b>	RESPONSE	EXPLANATION OF CONTROLS	SUBSTANTIATING DOCUMENT(S)
	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.	PLEASE RESPOND (Using Dropdown)		
	<b>MINIMUM REQUIRED LEVEL = PARTIALLY</b>			
18	<b>APPLICATION SOFTWARE SECURITY</b>	RESPONSE	EXPLANATION OF CONTROLS	SUBSTANTIATING DOCUMENT(S)
	Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.	PLEASE RESPOND (Using Dropdown)		
	<b>MINIMUM REQUIRED LEVEL = PARTIALLY</b>			
19	<b>INCIDENT RESPONSE AND MANAGEMENT</b>	RESPONSE	EXPLANATION OF CONTROLS	SUBSTANTIATING DOCUMENT(S)
	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.	PLEASE RESPOND (Using Dropdown)		
	<b>MINIMUM REQUIRED LEVEL = PARTIALLY</b>			

# ATTACHMENT 17



## RFP entitled: “Pharmacy Benefit Services for The Empire Plan, Student Employee Health Plan, and NYS Insurance Fund Workers’ Compensation Prescription Drug Programs”

20	PENETRATION TESTS	RESPONSE	EXPLANATION OF CONTROLS	SUBSTANTIATING DOCUMENT(S)
	<p>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.</p> <p><b>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.</b></p> <p><b>Additional Information for Vendors:</b></p> <ol style="list-style-type: none"> <li>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. <u>This should not be confused with vulnerability assessments which may be part of a penetration test but not a substitute for it.</u></li> <li>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.</li> <li>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.</li> <li>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:             <ol style="list-style-type: none"> <li>a) Network Testing.</li> <li>b) Cloud, Web and Mobile Application Testing (Where Applicable).</li> <li>c) Vulnerability Scanning.</li> <li>d) Exploitation.</li> <li>e) Remediation Plan.</li> </ol> </li> <li>5. Additional information             <ol style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>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.</li> </ol> </li> </ol>	<p>PLEASE RESPOND (Using Dropdown)</p>		
	<p><b>MINIMUM REQUIRED LEVEL = PARTIALLY</b></p>			