New York State Division of Homeland Security and Emergency Services Cybersecurity Services Agreement

This Agreement, made this _____day of _____, 20____, by and between the State of New York, acting by and through the New York State Division of Homeland Security and Emergency Services, having its principle place of business at the Harriman State Office Campus,1220 Washington Avenue, Building 7A, 7th Floor, Albany, New York 12226, hereinafter referred to as the "State" and _____, having its principal place of business located at_____, hereinafter referred to as "Recipient". Each party to this Agreement is referred to as a "Party" and collectively as the "Parties."

W I T N E S S E T H:

WHEREAS, pursuant to Executive Law §§ 709(2)(j) and (2)(o) the State maintains cybersecurity teams which assist local governments and State agencies and private entities with cyber security preparedness by conducting vulnerability assessments, network scans, penetration tests, phishing, examinations and/or analyses of information technology (hereinafter IT) networks and systems (hereinafter Cyber Services); and

WHEREAS, the Recipient is such an entity located in the State of New York that maintains various information technology (hereinafter IT) networks and systems[1] to provide its services; and

WHEREAS, the Recipient recognizes the need to maintain secure IT networks and systems;

WHEREAS, this Agreement includes Appendix "B" listing the suite of the State's Cyber Services available to Recipient; and

WHEREAS, the Recipient may request Cyber Services as referenced in Attachment "B" from the State following the process and procedure set forth in this Agreement;

NOW, THEREFORE, the State and the Recipient hereby agree as follows:

1. This Agreement includes the attached Appendix "A", Appendix "B," and any and all agreed to Scopes of Work and Rules of Engagement, which shall be incorporated into the terms of this Agreement by reference as though more fully set forth in their entirety herein.

2. The State's Cyber Services shall be available to Recipient for a three (3) year period commencing on [date] and shall end on [date]. Recipient is authorized to make multiple requests for the State's Cyber Services during this three (3) year period, subject to the State's agreement and approval.

3. The Parties shall set forth the specific Cyber Services agreed to be performed by the State for the benefit of the Recipient in a Scope of Work which shall be completed prior to the commencement of any work along with Rules of Engagement.

4. Recipient shall designate in writing, on its official letterhead, its authorized representative to select, identify, and notify the State of the specific Cyber Services requested and such authorized representative shall be authorized to execute Scopes of Work and Rules of Engagement and all related documents during the term of this Agreement on behalf of Recipient. Such Designation shall be notarized and may be amended and superseded at the discretion of the Recipient.

[1] IT networks and systems may include, but is not necessarily limited to desktops, laptops, servers, network information systems and other networked electronic devices.

5. Recipient hereby authorizes the State to access, use, and otherwise interact with its IT networks and systems, as specified in the Scope of Work, to conduct such vulnerability assessments, network scans, penetration tests, phishing, examinations and/or analyses as described in the attached Scope of Work and in accordance with the attached Rules of Engagement.

6. Recipient acknowledges and assumes all risks associated with the services performed under this Agreement including but not limited to the Cyber Services, as specified in the Scope of Work, or implementation of any State guidance which may result in a reduction of or interruption in the operation and function of some or all of Recipient's IT systems and networks during or after the Cyber Services as specified in the Scope of Work, or implementation of guidance, including, but not limited to the following risks: loss of host availability, loss of network availability, loss of data, corruption of data in transit, corruption of data at rest, corruption of data at use, network instability, and host instability. The State intends to use its best efforts to conduct the Cyber Services as specified in the Scope of Work, in a manner that minimizes risk and impact to the Recipient's IT systems and networks but makes no warranties with respect to the function or operation of Recipient's IT networks and systems before, during or after performing the Cyber Services. Recipient agrees to promptly notify the State's assigned engagement lead in the event that Recipient reasonably suspects that activities governed by this agreement may be having a negative impact on Recipient's networks, systems and / or personnel.

7. Except as may be required by applicable law or a court of competent jurisdiction in the State of New York, the State, its officers, agents, and employees, if any, will endeavor to use reasonable efforts to maintain the confidentiality of Recipient's IT system and network and information and data related thereto.

8. As an express condition of the State conducting its Cyber Services as specified in the Scope of Work, Recipient waives, releases and forever discharges the State from any and all negligence actions, causes of action, suits, judgments, damages, claims, costs, and demands whatsoever, in law, or equity, which the Recipient has, may have or will have against the State, its officers, agents, and employees, if any, of every kind and nature and relating to the Cyber Services performed by the State and/or, as specified in the Scope of Work.

9. Recipient shall be solely responsible and answerable in damages for any and all claims and causes of action arising out of or related to the vulnerability assessment, network scans, tests, examinations and/or analyses, as specified in the Scope of Work, activities conducted pursuant to this Agreement to the extent attributable to the Recipient or its employees and contractors. Recipient shall indemnify and hold harmless, the State, and its officers, agents, employees, and subcontractors, if any, from any negligence claims, suits, actions, damages, and costs (including reasonable attorney fees) of every kind and nature arising out of the performance of the Cyber Services as specified in the Scope of Work and related activities including any changes in the function or operation of Recipient's IT networks and systems and/or the disclosure of confidential information.

10. Recipient agrees to promptly notify necessary third parties, including but not limited to third-party system owners, of the State's activities and secure necessary third-party authorizations in a timely fashion. Recipient will bear the full responsibility for any liability that results from the failure to secure necessary third-party authorizations and waivers, and for any damage to third parties arising out of or related to the vulnerability assesment, network scans, tests, examinations and or analyses, as specified in Scope of Work, performed by the State.

11. This constitutes the entire agreement between the parties hereto and all previous communications, whether written or oral relating to the subject matter of this contract are hereby superseded. If any provision of this agreement is adjudged to be void or otherwise unenforceable, in whole or in part, such adjudication shall not affect the validity of the remainder of the agreement.

12. This constitutes the entire Agreement, including Appendix “A,” Appendix “B,” and any future Scope of Work and Rules of Engagement, between the parties hereto and no statement, promise, condition, understanding, inducement or representation, oral or written, expressed or implied, which is not contained herein shall be binding or valid and this Agreement shall not be changed, modified or altered in any manner except by an instrument in writing executed by both parties herein.

IN WITNESS WHEREOF, the Recipient has caused this instrument to be sealed and signed by Recipient or its duly authorized agent/officer, and the State has caused this instrument to be executed by its duly authorized officer.

NYS Division of Homeland Security and Emergency Services	Recipient Name
By: _____	By: _____
Director or Authorized Designee	(Name and Title of authorized representative)
NYS Division of Homeland Security and Emergency Services	

Acknowledgement Clause

State of New York)
)ss.
County of_____)
On this _____ day of _____ , 20__, before me, the undersigned, personally appeared _____ , personally known to me or proved to me on the basis of satisfactory evidence to be the individual(s) whose name(s) is(are) subscribed to the within instrument and acknowledged to me that he/she/they executed the same in his/her/their/ capacity(ies), and that by his/her/their signature(s) on the instrument, the individual(s), or the person upon behalf of which the individual(s) acted, executed the instrument.

Appendix B:

Recipient, please initial the services that you would like to have covered under this agreement:

____ 1. Phishing Assessment – Requesting this service will authorize DHSES to simulate an email-based phishing attack to assess the effectiveness of your email security training along with a separate training to educate users on how to spot phishing messages. CIRT will then deliver a report showing how many users were deceived by the phishing emails, to what extent they interacted with the suspect emails, and how many completed the training.

____ 2. Cyber Risk Assessment – Requesting this service will authorize DHSES to perform a Cybersecurity Risk Assessment for your organization. This assessment may include one or more of the following activities: vulnerability scanning of publicly accessible IT devices and internal IT devices, Open-Source Intelligence gathering, a review of your internal policies related to Cyber Security, and interviews with some of your personnel to understand the implementation level of your internal controls and policies. It will culminate in a final report that contains action-oriented, prioritized findings. The specifics of this program are laid out in the Risk Assessment Rules of Engagement and Scope of Work documents and must be completed prior to the start of any activity.

_____3. Penetration Testing – Requesting this service will authorize DHSES to simulate a cyber attack against your local infrastructure. Any identified vulnerabilities will be exploited to fully demonstrate the impact and any exploit chain that is exposed by that vulnerability. Although no destructive attacks will be used by DHSES staff, any potentially destructive vulnerabilities (Denial of Service, Data destruction, etc) may be noted during the assessment. It will culminate in a final report that contains action-oriented, prioritized findings. Some of the findings will include steps to replicate as appropriate so that your staff my test any corrective actions / mitigations that they apply as a result of the report. The specifics of each test will be laid out in the Pentesting Rules of Engagement and Scope of Work documents and must be completed prior to the start of any activity.

_____4. Adhoc Vulnerability Scans – These vulnerability scans will be performed against publicly accessible systems and services at your request. While they are not a replacement for a routine vulnerability scanning program, they can be used during a potential Cyber Incident or to test new, publicly accessible applications or services. The scanners used by CIRT include but are not limited to opensource scanners such as NMAP and commercial products such as Nessus.