CYBER INFORMATION SHARING AND COLLABORATION AGREEMENT
Between
the NEW YORK STATE OFFICE OF INFORMATION TECHNOLOGY SERVICES, NEW YORK STATE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES

And
Albany County

X050124

This Agreement, made this _____day of _____, 20____, by and between the New York State Office of Information Technology Services with offices at Empire State Plaza, Swan Street Building Core 4, Albany, New York 12223 ("ITS"), and the New York State Division of Homeland Security and Emergency Services ("DHSES"), having its principle place of business at the Harriman State Office Campus,1220 Washington Avenue, Building 7A, 7th Floor, Albany, New York 12226 (collectively referred to as the "State"), and Albany County, having its principal place of business located at_____, hereinafter referred to as "Participating Entity." Each party to this Cyber Information Sharing and Collaboration Agreement ("CISCA or Agreement") is referred to individually as a "Party" and collectively as the "Parties."

WITNESSETH:

WHEREAS, there is established within the State a Joint Security Operations Center ("JSOC") to serve as the round the clock operational center for the purposes of sharing of cyber threat information that is uniquely positioned as a sharing hub to integrate information and facilitate operational collaboration from multiple sources; and

WHEREAS, the NY Security Operations Center Initiative ("hereafter, "NY SOC") is a one-of-a kind cooperative approach between State and local governments to enhance collective cybersecurity and risk management capabilities and provide Participating Entities with actionable information to prevent, detect, respond to and recover from cyber attacks; and

WHEREAS, DHSES is required to work with federal, state, local and private entities to protect the State's critical infrastructure from cyber threats and vulnerabilities and to coordinate and facilitate information and intelligence sharing amongst these entities to assist in the early identification of and response to natural and manmade disasters; and

WHEREAS, ITS is responsible for protecting New York State Government's cyber security infrastructure and does so by employing a multi-faceted approach that includes coordinating policies, standards and programs on cybersecurity across the State, partnering with State agencies and law enforcement, monitoring the State's technology assets and responding to abnormalities and threats to their systems; and

WHEREAS, the Participating Entity provides vital services to the residents of New York State within its jurisdictional boundaries; and
WHEREAS, the Participating Entity desires to provide the State with Confidential Information or Cyber Information and logging data to contribute to an unprecedented level of visibility into potential threats across the State and increase efficiency in detecting and responding to cybersecurity events and incidents; and

WHEREAS, the State desires to receive, analyze, integrate and disseminate Confidential Information and Cyber Information from the Participating Entity and improve the State's collective cybersecurity and risk management capabilities; and

WHEREAS, the State is equipped to facilitate the exchange of Confidential Information and Cyber Information and offer a variety of services to Participating Entities, and

NOW THEREFORE, in furtherance of the above-referenced objectives the Parties desire to enter into this Agreement to share cybersecurity information and engage in collaboration activities as part of the NY SOC.

Definitions

"**Authorized Activities**:" Means:

(i) A Cybersecurity Purpose; or
(ii) The purpose of identifying a cybersecurity threat, including the source of such cybersecurity threat; or a security vulnerability;
(iii) The purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or use of a weapon of mass destruction;
(iv) The purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety.

"**Confidential Information:**" Means any non-public information that a Party ("Disclosing Party"), regardless of form or medium of disclosure (e.g., verbal, hard copy, or electronic) or source of information (e.g., ITS, other state agencies, electronic systems, federal government, or third-party contractors) provides to the other Party or Parties, its agents, employees, officers, partners, or subcontractors ("Receiving Party") or which the Receiving Party obtains, discovers, derives, or otherwise becomes aware of as a result of performance of this Agreement.

"**Cyber Information:**" Means information owned or derived by a Party relating to cyber intelligence, indicators of compromise, indicators of cyber threat, cybersecurity investigative information, defensive measures being taken during an ongoing or imminent threat, and other such information relating to cybersecurity including all types of security log data and telemetry from information systems and infrastructure.

"**Cybersecurity Purpose**:" Means the purpose of protecting an information system (of a Party) or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

"**Cybersecurity Threat**:" Means an action that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system; but does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

"**Participating Entity**:" Means a New York State local government that has entered into this Agreement that discloses Confidential Information or Cyber Information and receives Cyber Information from the State.

"Security Incident:" Means a cyber event that a Party believes has compromised or may compromise the security, confidentiality, availability or integrity of its data, systems, networks, or other information technology related assets.

1. **Purpose**

This Agreement sets forth the terms and conditions for the sharing of Confidential Information and Cyber Information and collaborative activities to achieve a Cybersecurity Purpose, including Participating Entities' participation in such activities. This Agreement enables the State and the Participating Entity to share Confidential Information and Cyber Information and engage in analytical collaboration activities, including technical exchanges associated with cybersecurity risks.

2. **Participating Entity**

2.1 The Participating Entity shall designate Points of Contact, for both Information Technology and cybersecurity related issues, who will be involved in the receipt, dissemination and accountability of the handling Confidential Information or Cyber Information on the effective date of this Agreement and annually thereafter.

2.2 The Participating Entity's Points of Contact shall attend any State training on submission, protection and handling of Confidential Information or Cyber Information.

2.3 The Participating Entity shall submit to, and continuously update as the information changes, the State a list of Participating Entity's contractors whose contracts include protecting the Participating Entity's information and information systems and who therefore may participate in operational data flow and analytic collaboration activities offered by the State.

2.4 The Participating Entity may request: (A) additional information related to risk mitigation efforts; (B) collaboration regarding cybersecurity risks, or (C) briefings of specific and relevant threat topics or incidents.

2.5 The Participating Entity may supply Confidential Information or Cyber Information for a Cybersecurity Purpose. The Participating Entity may or may not own the Confidential

Information or Cyber Information or be the source of the Confidential Information or Cyber Information it produces.

2.6 The Participating Entity shall use reasonable efforts to ensure that Confidential Information and Cyber Information shared is accurate at the time that it is supplied.

2.7 The Participating Entity shall use reasonable efforts to remove from Confidential Information or Cyber Information any information not directly related to a Cybersecurity Threat that the Participating Entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual.

2.8 The Participating Entity agrees that the State may disclose, pursuant to legal and regulatory limitations, use and retain Confidential Information and Cyber Information provided to the State for an Authorized Activity.

2.9 The Participating Entity may disclose Confidential Information or Cyber Information to their third-party representatives who have a legitimate business need to know or use such Confidential Information or Cyber Information for purposes of aiding in authorized activities, provided that such third-party representative (1) is advised by the Participating Entity of the sensitive and confidential nature of such Confidential Information or Cyber Information; and (2) agrees to comply with the provisions of this Agreement as if they were a Party.

2.10 The Participating Entity agrees that, in the event that it discloses Confidential Information and Cyber Information by mistake or in error, it shall promptly notify the State and take all reasonable steps to mitigate, including sending a versioning update, as it is able.

2.11 The Participating Entity shall share Confidential Information or Cyber Information in accordance with State guidance.

2.12 The Participating Entity shall receive Confidential Information and Cyber Information in accordance with State guidance that identifies how Participating Entities can receive Confidential Information or Cyber Information.

2.13 The Participating Entity shall use Confidential Information and Cyber Information for Authorized Activities.

2.14 The Participating Entity shall provide, if requested by the State, a written description of the technical measures and/or protections it has implemented based on State-provided Confidential Information and Cyber Information.

2.15 The Participating Entity shall ensure that any risk mitigation efforts that are based on State-provided Confidential Information and Cyber Information do not initiate communications with related threat resources defined within State provided Confidential Information and Cyber Information without first coordinating such efforts with the State unless expressly prohibited from doing so by a law enforcement agency with proper jurisdiction.

2.16 The Participating Entity shall not disclose, advertise, or publicize, absent legal compulsion or other legal requirement, the identity of any Participating Entity absent that Participating Entity's prior written consent. If Participating Entity is legally compelled to disclose such information, it shall promptly notify the subject of the disclosure unless prohibited by court order.

2.17 The Participating Entity shall work with the State to implement and maintain systems responsible for the aggregation and transmission of Confidential Information and Cyber Information to the State in a robust and secure manner.

2.18 The Participating Entity shall remain responsible for meeting any and all data retention and compliance requirements outside of the environment.

2.19 The Participating Entity shall be responsible for resolving any disruptions in Confidential Information or Cyber Information transmission to the State. Failure to do so may impact the Participating Entity's benefit from State services.

3. NYS Responsibilities

3.1 The NY SOC is a State-provided interface for the sharing of information related to cybersecurity threats, incidents analysis and warnings for State and local governments. Confidential Information and Cyber Information received by the State will be accessible by all NY SOC personnel. All NY SOC personnel who may have access to Confidential Information and Cyber Information are subject to a formal background check requirement compliant with the FBI's Criminal Justice Information Services (CJIS) requirements and must take training consistent with the State's federal obligations. In addition to these requirements, vendor partners of the State who may need access to Confidential Information and Cyber Information to assist the NY SOC personnel in carrying out the services described in this Agreement, are also subject to certain non-disclosure agreements.

3.2 The State shall use Confidential Information and Cyber Information solely for Authorized Activities.

3.3 The State may incorporate the non-attributable and anonymized threat, vulnerability, or risk management portion of Confidential Information and Cyber Information submitted by a Participating Entity into analytical products.

3.4 The State shall provide an integrated analysis of Confidential Information and Cyber Information and coordinate and facilitate information sharing among Participating Entities to assist in the early detection and response to cybersecurity threats and security incidents.

3.5 The State may share Confidential Information and Cyber Information with Participating Entities and other entities but shall anonymize the identity of the Participating Entity from any Confidential Information and Cyber Information before sharing with other Participating Entities and other entities, unless the Participating Entity consents affirmatively to disclosure of its identity.

3.6 The State may disclose Confidential Information or Cyber Information to their third-party representatives who have a legitimate business need to know or use such Confidential Information or Cyber Information for purposes of aiding in Authorized Activities, provided that such third-party representative (1) is advised by the State of the sensitive and confidential nature of such Confidential Information or Cyber Information; and (2) agrees to comply with the provisions of this Agreement as if they were a Party.

3.7 The State shall coordinate periodic, relevant, technical exchanges, analytical collaboration, briefings and discussions to support the program activities described in this Agreement as appropriate.

3.8 The State shall respond to requests for information, collaboration, or briefings submitted by a Participating Entity, as appropriate and in accordance with State guidance.

3.9 The State shall maintain the mechanisms for ingesting Confidential Information and Cyber Information from Participating Entities. This pertains to all systems within the NY SOC environment.

3.10 The State shall develop guidance based on industry best practice to provide Participating Entities with instructions on how they must configure and support a secure and reliable transfer of Confidential Information and Cyber Information to the State.

4**. Handling of Information**

a. Confidentiality Obligations. Each Party will:
   i. Hold all Confidential Information and Cyber Information provided by the other Party in strict confidence, except as otherwise expressly permitted under this Agreement;
   ii. Not disclose Confidential Information or Cyber Information of the other Party to any third-parties except to those who are subject to the same obligations as set forth in this Agreement, or as otherwise set forth in this Agreement;
   iii. Not process Confidential Information or Cyber Information of the other Party in any way not authorized by this Agreement;
   iv. Limit reproduction of the other Party's Confidential Information and Cyber Information to a need only basis;
   v. When Confidential Information or Cyber Information is shared, not disclose any Confidential Information or Cyber Information that may be used to identify the other Party;
   vi. In the event of an unauthorized or inadvertent use or disclosure of, or access to Confidential Information and Cyber Information, shall without unreasonable delay upon discovery that an unauthorized disclosure or loss has occurred, notify the other Party in writing and shall ensure a proper record of such unauthorized or inadvertent use, disclosure or access is kept and immediately provided to the other Party. The Parties shall also assist in any subsequent investigation of

the unauthorized or inadvertent use, disclosure or access and mitigate any possible resulting damages of same. A record required under this provision shall include, at a minimum, the following:

1. Date of the unauthorized use or inadvertent disclosure;
2. Name of the recipient of the unauthorized use or inadvertent disclosure;
3. Address of the recipient of the unauthorized use or inadvertent disclosure, if known;
4. Brief description of the Confidential Information or the Cyber Information used or disclosed;
5. Any remedial measures taken to retrieve or otherwise repossess such Confidential Information or Cyber Information; and
6. All other details required or necessary for the Party disclosing the Confidential Information or Cyber Information to know when and how such unauthorized disclosure was made and what mitigating steps are being undertaken or recommended to remedy.

vii. Take steps to avoid publication or dissemination of the Confidential Information and Cyber Information using at least the same degree of care as the Parties would use with respect to their own Confidential Information and Cyber Information; and

viii. At all times, have the right to request reasonable further assurances that the foregoing restrictions and protections concerning Confidential Information and Cyber Information are being observed, and the Party receiving the request must promptly provide the assurances.

b. <u>Exceptions Allowing Parties to Disclose Certain Confidential Information and Cyber Information</u>

i. The confidentiality obligations in this Agreement do not apply to the extent that the Party receiving the Confidential Information or Cyber Information can demonstrate or establish by written evidence that: (1) the Confidential Information or Cyber Information became part of the public domain other than through actions that constitute a breach of this Agreement or fault on the part of the Receiving Party; (2) the Confidential Information or Cyber Information was lawfully obtained by the Receiving Party from a source other than the Disclosing Party free of any obligation to keep it confidential; (3) Receiving Party developed such information independently of and without reference to any Confidential Information or Cyber Information of the Disclosing Party (Receiving Party shall bear the burden of proving such independent development); (4) the Disclosing Party expressly authorized disclosure of the Confidential Information or Cyber Information; (5) the Confidential Information or Cyber Information is required to be disclosed pursuant to law, regulation, judicial or administrative order, or request by a governmental or other entity authorized by law to make such request; provided, however, that the

Receiving Party shall comply with Section 4(b)(ii) (Disclosure if Legally Compelled) below; or (6) the Disclosing Party, in its sole discretion, agrees that the Confidential Information or Cyber Information has been anonymized to remove personal identifying information or information not otherwise disclosable under existing law.

ii. Disclosure if Legally Compelled

1. Notwithstanding anything herein, in the event that a Party receives notice that it has, will, or may become compelled, pursuant to applicable law, regulation, or legal process to disclose any Confidential Information or Cyber Information (whether by receipt of oral questions, interrogatories, requests for Confidential Information or Cyber Information or documents in legal proceedings, Freedom of Information Law ("**FOIL**") requests, subpoenas, civil investigative demands, other similar processes, or otherwise), that Party shall, except to the extent prohibited by law, within two (2) business days of receipt of such notice, notify the other Party, orally and in writing, of the pending or threatened compulsion. In performing their obligations and exchanging information under this Agreement the Parties are acting in their common interests, each Party will maintain and support the attorney-client and work product privilege if asserted by the other Party.
2. To the extent permitted by law, the Parties will coordinate and cooperate with each other in advance of any disclosure, in order to undertake any lawfully permissible steps to reduce and/or minimize the extent of Confidential Information or Cyber Information that must be disclosed.
3. To the extent permitted by law, the Parties will have the right to seek an appropriate protective order or other remedy reducing and/or minimizing the extent of Confidential Information or Cyber Information that must be disclosed.
4. Upon determination that Confidential Information or Cyber Information must be disclosed pursuant to this section, the Party receiving the request and its third-party representatives shall disclose only such Confidential Information or Cyber Information that they are legally required to disclose in order to comply with such applicable law or regulation or legal process (as may be affected by any protective order or other remedy obtained by a Party). The Party and its third-party representatives shall use all reasonable efforts to ensure that all Confidential Information or Cyber Information that is so disclosed will be accorded confidential treatment.

c. Security

i. The Parties shall store Confidential Information and Cyber Information in

a secure fashion at a secure location that is not accessible to any person or entity not authorized to receive the Confidential Information or Cyber Information under the provisions of this Agreement;

ii. Temporary Suspension of Obligations. At any time, a Party may suspend performance of one or more of its obligations under this Agreement without terminating in the event of an actual or suspected Security Incident or a security breach of a third-party that may affect the suspending Party. The suspending Party will provide notice of the suspension as soon as practicable under the circumstances. Notwithstanding the foregoing, unless legally compelled without the possibility of contractual waiver, this Section 4(c)(ii) will not apply to Sections 4(a) and 13 of this Agreement.

d. Coordination of Public Statements

i. Any public references to or descriptions of the existence of or nature of this Agreement, the program activities undertaken under this Agreement by either Party, or any Analytical Products produced jointly by the Parties under this Agreement shall be done only after coordination, in writing between the Parties.

ii. Each Party shall receive written approval from the other Party before publishing in a journal or similar publications any Confidential Information or Cyber Information provided by the other Party under this Agreement or first created or developed jointly under this Agreement.

5. **TERM**

The term of this Agreement shall be for a period of three years and will automatically renew annually thereafter unless a Party gives notice of termination as required under Section 6 herein. This Agreement reflects the Parties desire to enter into a long-term relationship to enhance collective cybersecurity and risk management capabilities.

6. **TERMINATION**

a. For Convenience

Each Party retains the right to cancel the Agreement without cause and without penalty, provided that at least ninety (90) calendar days' notice of the Party's intent to cancel is given. This provision should not be understood as waiving a Party's right to terminate the Agreement for cause or stop work immediately for unsatisfactory work, but is supplementary to that provision.

b. For Cause

For any material breach or failure of performance of the Agreement by a Party, the other Party may provide written notice of such breach or failure. A Party may terminate the Agreement if the other Party does not cure such breach or failure within thirty (30) calendar days after the giving of written notice to cure. No delay or omission to exercise any right, power, or remedy accruing to a Party upon breach or default by the other Party under the Agreement shall impair any such right, power or remedy, or shall be construed as a waiver of any such breach or default, or any

similar breach or default thereafter occurring nor shall any waiver of a single breach or default be deemed a waiver of any subsequent breach or default. All waivers must be in writing.

c. Termination Notice
Notices required by this section shall be delivered to the other Party in writing, pursuant to the Notice provisions of this Agreement.

d. Data Migration and Destruction
Upon expiration or termination of this Agreement, the Parties agree to return each respective Party's Confidential Information and Cyber Information within a period of ninety (90) days following expiration or termination, including metadata and attachments, in a mutually agreed upon, commercially standard format. Thereafter, except for data required to be maintained by federal, state, and local laws, rules, regulations, ordinances, policies, standards, or guidelines or this Agreement, each Party shall destroy the other Parties' Confidential Information and Cyber Information from its systems and wipe all its data storage devices to eliminate any and all Confidential Information and Cyber Information from its systems. The sanitization process must be in compliance the NYS Security Standard, NYS-S13-003, available at https://www.its.ny.gov/document/sanitizationsecure-disposal-standard, and other sanitization and disposal standards where required by State policy or law. If immediate purging of all data storage components is not possible by a Party, that Party will certify that any Confidential Information or Cyber Information remaining in any storage component will be safeguarded to prevent unauthorized disclosures until such purging is possible. The non-purging Party must then certify to the other Parties, in writing, that it has complied with the provisions of this paragraph including providing any supporting documentation as required.

7. **WARRANTIES**
To the extent permitted by law, there are no other express or implied warranties or conditions, including warranties or conditions of merchantability and fitness for a particular purpose.

8. **NO PERSONAL LIABILITY**
No commissioner, officer, agent, or employee of either Party shall be held personally liable under any provision of this Agreement or because of its execution or attempted execution or because of any breach or alleged breach hereof.

9. **NO THIRD-PARTY RIGHTS**
Nothing in the Agreement shall create or give to third parties any claim or right of action against the Participating Entity or the State beyond such as may legally exist irrespective of the Agreement.

10. **NOTICES**
a. All notices permitted or required hereunder shall be in writing and shall be transmitted either:

i. Via certified or registered United States mail, return receipt requested;
ii. By facsimile transmission;
iii. By personal delivery;
iv. By expedited delivery service; or

v. By email.

Such notices shall be addressed as follows or to such different addresses as the parties may from time to-time designate:

ITS:

NYS Office of Information Technology Services
Division of Legal Affairs
Empire State Plaza, PO Box 2062 Albany, NY 12220-0062
Attn: Chief General Counsel
Email: its.sm.dla@its.ny.gov

DHSES:

NYS Division of Homeland Security and Emergency Services
Cyber Incident Response Team
1220 Washington Ave, Bldg 7A
Albany, NY 12226
Attn: CIRT Director
Email: CIRT@dhses.ny.gov

With a copy to:

NYS Division of Homeland Security and Emergency Services
Office of Counsel
1220 Washington Ave, Bldg 7A
Albany, NY 12226
Attn: Deputy Counsel
Email: thomas.mccarren@dhses.ny.gov

Participating Entity
Name:
Title:
Address:
Telephone Number:
E-Mail Address:

b. Any such notice shall be deemed to have been given either at the time of personal delivery or, in the case of expedited delivery service or certified or register United States mail, as of the date of first attempted delivery at the address and in the manner provided, or in the case of facsimile transmission or email, upon receipt.

11. **AMENDMENTS**
This Agreement may be amended, modified or superseded, and the terms or conditions hereof may be waived only by a written instrument signed by the State and Participating Entity.

12. **DISPUTE RESOLUTION**
The Parties agree that prior to the commencement of any legal proceeding, the Parties shall, in good faith, attempt to resolve any disputes that arise from this Agreement. The Party commencing a dispute shall do so by submitting a description of the dispute in writing to the other Party's designated single point of contact. The following escalation procedures shall be followed:

a. The Parties designated single points of contact shall attempt to amicably resolve the dispute within ten (10) business days, or as otherwise agreed to by the Parties.

b. If the Parties designated single points of contact are unable to resolve the dispute, such dispute will be submitted to the ITS Chief Information Officer, the Commissioner of DHSES, and the Participating Entity's chief executive officer for resolution.

13. **INDEMNIFICATION**
a. Subject to the availability of lawful appropriations, the Participating Entity shall hold the State, its officers, agents, and employees harmless from and indemnify it for any final judgment of a court of competent jurisdiction or amounts paid in settlement of a third-party claim to the extent attributable to the negligence of the Participating Entity or of its officers or employees when acting within the course and scope of their employment.

b. Subject to the availability of lawful appropriations consistent with Section 8 of the State Court of Claims Act, the ITS and/or DHSES shall hold the Participating Entity harmless from and indemnify it for any final judgment of a court of competent jurisdiction or amounts paid in settlement of a third-party claim to the extent attributable to the negligence of the ITS and/or DHSES or of its officers or employees when acting within the course and scope of their employment.

14. **GENERAL PROVISION AS TO REMEDIES**
The Parties may exercise their respective rights and remedies at any time, in any order, to any extent, and as often as deemed advisable, without regard to whether the exercise of one right or remedy precedes, concurs with or succeeds the exercise of another. A single or partial exercise of a remedy shall not preclude a further exercise of the right or remedy or the exercise of another right or remedy from time to time. No delay or omission in exercising a right or remedy, or delay, inaction, or waiver of any event of default, shall exhaust or impair the right or remedy or constitute a waiver of, or acquiescence to, an event otherwise constituting a breach or default under the Agreement.

15. **ADDITIONAL REMEDIES**
In addition to any other remedies available to the Parties under this Agreement and state and federal law for the other Party's default, a Party may choose to exercise some or all of the following:
• Pursue equitable remedies to compel a Party to perform;
• Require a Party to cure deficient performance or failure to meet any requirements of the Agreement.

16. **INDEPENDENT CONTRACTORS**
Nothing in this Agreement shall be construed to create any partnership, joint venture or agency relationship of any kind. Neither Party has any authority under this Agreement to assume or create any obligations on behalf of or in the name of the other Party or to bind the other Party to any contract, agreement or undertaking with any third party.

17. **ASSIGNMENT**
The State may assign this Agreement, including all right and responsibilities to any successor NYS entity. The Participating Entity will be provided notice of any assignment. The Participating Entity may assign this Agreement as required by operation of law or with the consent of the State, such consent shall not be unreasonably withheld. Such assignment may be subject to approval by OSC, if applicable.

18. **NON-WAIVER**
The failure by any Party to insist on performance of any term or condition or to exercise any right or privilege included in this Agreement shall not constitute a waiver of same unless explicitly denominated in writing as a waiver and shall not thereafter waive any such term or condition and/or any right or privilege. No waiver by any Party of any breach of any term of this Agreement shall constitute a waiver of any subsequent breach or breaches of such term.

19. **ENFORCEABILITY/SECTION HEADINGS**
In the event any clause, or any part or portion of any clause of this Agreement shall be held to be invalid, void, or otherwise unenforceable, such holding shall not affect the remaining part or portions of that clause, or any other clause hereof. The section headings in this Agreement are inserted only as a matter of convenience and for reference and in no way define, limit or fully describe the scope or intent of any provision of this Agreement.

20. **JURISDICTION**
This Agreement shall be construed according to the laws of the State of New York, except where the federal supremacy clause requires otherwise, and all claims concerning this Agreement shall be determined in a court of competent jurisdiction in the county of the state of New York in which the claim is alleged to have arisen.

21. **EXECUTION**
By execution, delivery and performance of this Agreement, each party represents to the other that it has been duly authorized by all requisite action on the part of the Participating Entity and the State respectively. This Agreement constitutes the legal, valid, and binding obligation of the Parties hereto.

22. **ENTIRE AGREEMENT**
This Agreement represents the entire understanding and agreement between the Participating Entity, ITS, and DHSES with respect to the subject matter hereof, and supersedes all other negotiations, understandings and representations (if any) made by and between such Parties.

23. ORDER OF PRECEDENCE
The provisions of this Agreement and, if applicable, the Intergovernmental Agreement for the Provision of Endpoint Protection and Response Services (EDR Agreement) shall be construed and interpreted as consistent whenever possible. In the event of a conflict between the terms of this Agreement and the EDR Agreement, the terms of this Agreement shall take precedence.

IN WITNESS WHEREOF, this Contract has been duly executed on the date and year set out below.

By: _____

Name: _____

Title: _____

Date: _____, 20__

CORPORATE ACKNOWLEDGMENT STATE OF _____} ss.: COUNTY OF _____} On the _____ day of _____ in the year 20__, before me personally appeared: _____, known to me to be the person who executed the foregoing instrument, who, being duly sworn by me did depose and say that his/her place of business is at _____, Town/City of _____, County of _____ , State of _____; and further that s/he is the _____ of _____ , the corporation described in said instrument; that, by authority of the Board of Directors of _____ , s/he is authorized to execute the foregoing instrument on behalf of _____for purposes set forth therein; and that, pursuant to that authority, s/he executed the foregoing instrument in the name of and on behalf of said corporation as the act and deed of said corporation.

_____
Notary Public

NEW YORK STATE OFFICE OF INFORMATION TECHNOLOGY SERVICES By: _____ .

Name: _____

Title: _____

Date: _____, 20__

NEW YORK STATE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES
By: _____

Name: _____

Title: _____

Date: _____, 20__