INTERGOVERNMENTAL AGREEMENT FOR THE PROVISION OF ENDPOINT PROTECTION AND RESPONSE SERVICES (Phase II)

BETWEEN

THE NEW YORK STATE OFFICE OF INFORMATION TECHNOLOGY SERVICES,

THE NEW YORK STATE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES

AND

The City of Oneida

X052084

This Intergovernmental Agreement ("IA") is entered into by and among the New York State Office of Information Technology Services ("ITS"), the New York State Division of Homeland Security and Emergency Services ("DHSES"), ITS and DHSES collectively referred to herein as the "State," and the entity identified on the signature page of this IA which is a political subdivision, municipal corporation, or public authority as defined by the laws of the State of New York ("Participating Entity"). By entering into this IA, the Participating Entity acknowledges that it has the legal authority to enter into this IA and that the individual executing this IA has been duly authorized to execute the IA. Each party to this IA is referred to individually as a "**Party**" and collectively as the "**Parties**."

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 cyber security 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, DHSES is responsible for working 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 man-made disasters; and

WHEREAS, the Participating Entity provides vital services to residents of New York State and within its jurisdictional boundaries; and

WHEREAS, the Parties remain committed to ensuring the safety of their respective critical infrastructure by investing in strategic collaborations and technology for strengthening cyber security and resiliency in the face of evolving threats; and

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 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, "NYSOC") 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, increasingly sophisticated cyber-attacks on governmental entities as well as unauthorized access to their systems may compromise the security and integrity of government data, disrupt operations and services and damage critical infrastructure, thereby risking the health and welfare of the public; and

WHEREAS, the Parties recognize that deployment and use Endpoint Detection and Response (EDR) software, and rapid information sharing are foundational components of a sound cybersecurity program; and

WHEREAS The estimated total value of the endpoint detection licenses which is provided at no cost to the Participating Entity over the term of the Intergovernmental Agreement (3 years) is $61,666.50 .

NOW THEREFORE, in consideration of the foregoing, the Parties hereby agree as follows:

1. PURPOSE AND BENEFITS

The purpose of this Intergovernmental Agreement is to allow Participating Entities to access EDR software for better proactive security collaboration on threat intelligence amongst New York State and political subdivisions of the State.

Taking advantage of economies of scale and the State's purchasing power, the State has arranged for the Participating Entity to receive EDR software at no cost. Additionally, as part of that arrangement, the software provider or its affiliates will work directly with the Participating Entity to deploy the EDR solution within the Participating Entity's environment and provide training to assist the Participating Entity with using the EDR software.

2. DEFINITIONS

"**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 ("**Recipient**") or which the Recipient obtains, discovers, derives, or otherwise becomes aware of as a result of performance of this IA.

"**Cyber Information**" means information owned or derived by a Party relating to cyber intelligence, indicators of compromise, indicators of cyber threat, cyber security investigative information, defensive measures being taken during an ongoing or imminent threat, and other such information relating to cyber security.

"EDR software data" means data derived from an endpoint security solution that continuously monitors endpoint devices to detect and respond to cyber security incidents that is shared through the software provider to the NYSOC.

"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.

"**Affected Party**" means a Party that is affected by a Security Incident.

3. INTERGOVERNMENTAL AGREEMENT

The IA between the Parties consists of the following documents listed below in the following order of precedence:

a. Appendix A – Standard Clauses for All New York State Contracts
b. This IA document setting forth the final agreement between the Parties, including all attachments, appendices, and exhibits contained herein.

4. SERVICES

a. Obligations of the State:
    i. Facilitate and cover the cost of licensing for Endpoint Detection and Response (EDR) software for Participating Entity endpoints. The EDR software will be provided to the Participating Entity directly from the software provider.
    ii. Provide services, as selected by the Participating Entity, as described in Attachment A.
b. Obligations of the Participating Entity:
    i. Participating Entity will be responsible for providing a technical lead with access to deploy the EDR software on end points and sufficient IT staff to facilitate the deployment of this software in their environment.
    ii. Participating Entity agrees to abide by the EDR software provider's terms and conditions as agreed to between the State and the EDR software provider regarding use of the software and agrees to remain solely responsible for its use and configuration of the EDR software.
    iii. Participating Entity agrees to maintain and update the EDR software on their systems, including working with the EDR software provider directly to address any issues that arise from the software.
    iv. Participating Entity agrees that the EDR software will be configured to provide alerts to the NYSOC to contribute to the creation and monitoring of a statewide view of cybersecurity threats.

v. Participating Entity agrees to provide NYSOC a list of contacts and contact information for notification in the event of alerts or other information related to the service. Participating Entity agrees to provide updates to the list as needed.

vi. Participating Entity agrees to promptly notify all relevant entities, including but not limited to third-party system owners, of the State's activities and secure all necessary approvals, authorizations, or waivers in a timely fashion. Participating Entity will bear the full responsibility for all costs for obtaining such approvals, authorizations, or waivers, and any liability that results from the failure to secure, necessary approvals, authorizations or waivers, and for any damage to third parties arising out of or related to the products and services provided and/or performed by the State pursuant to this Section 4, including any intentional or negligent act or omission.

5. CONSIDERATION

The State agrees to provide the EDR software to the Participating Entity at no cost in exchange for the Participating Entity's agreement to share the EDR software data with the NYSOC to increase the State's visibility of the cyber threat landscape across the various state entities and political subdivisions, which will enhance the State's ability to quickly and more accurately respond to cybersecurity threats.

6. TERM

The initial term of the IA shall be for a period of three (3) years beginning on the effective date and will be automatically renewed for additional twelve (12) month terms based upon approval of funding in the State budget and approval of the New York State Office of the State Comptroller, if applicable The Parties agree that should funding for this initiative not be appropriated in a State budget, the IA shall terminate with ninety (90) days prior notice required. The effective date of this IA shall be the date of approval of the IA by the New York State Office of the State Comptroller, if applicable, otherwise, this IA shall be effective as of the date of the later signature of this IA.

7. TERMINATION

a. **For Convenience**

Each Party retains the right to cancel the IA 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 IA 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 IA by a Party, the other Party may provide written notice of such breach or failure. A Party may terminate the IA 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 IA 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 IA.

d. **Data Migration and Destruction**

Upon expiration or termination of this IA, 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 IA, 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 NYSOC policy or law. If immediate purging of all data storage components is not possible by a Recipient, that Recipient 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 Recipient 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.

8. 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.

9. NO PERSONAL LIABILITY

No commissioner, officer, agent, or employee of either Party shall be held personally liable under any provision of this IA or because of its execution or attempted execution or because of any breach or alleged breach hereof.

10. THIRD PARTY DATA SHARING

EDR software data received by the NYSOC will be accessible by all NYSOC personnel from various partner entities, including New York State and New York City. Any NYSOC personnel who may have access to EDR Data, 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 these entities who may need access to EDR data, Confidential Information, and Cyber Information to assist the NYSOC personnel in carrying out the services described in this IA, are also subject to certain non-disclosure agreements. The NYSOC personnel may share anonymized data with participating entities and other entities that enter into cyber information sharing agreements with the State.

11. CONFIDENTIAL AND CYBER INFORMATION SHARING

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 Section 11;
   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 Section 11, or as otherwise set forth in this Section 11;
   iii. Not process Confidential Information or Cyber Information of the other Party in any way not authorized by this IA;
   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:
      a. Date of the unauthorized use or inadvertent disclosure;
      b. Name of the recipient of the unauthorized use or inadvertent disclosure;
      c. Address of the recipient of the unauthorized use or inadvertent disclosure, if known;
      d. Brief description of the Confidential Information or the Cyber Information used or disclosed;

e. Any remedial measures taken to retrieve or otherwise repossess such Confidential Information or Cyber Information; and
f. 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. Exceptions Allowing Parties to Disclose Certain Confidential Information and Cyber Information

i. The confidentiality obligations in this Section 11 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 IA or fault on the part of Recipient; (2) the Confidential Information or Cyber Information was lawfully obtained by Recipient from a source other than the Disclosing Party free of any obligation to keep it confidential; (3) Recipient developed such information independently of and without reference to any Confidential Information or Cyber Information of the Disclosing Party (Recipient 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 Recipient shall comply with Section 11(b)(iii)(3) (Disclosure if Legally Compelled) below; (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; or (7) it is a third party as described in Section 10 above for which sharing Confidential Information or Cyber Information is necessary to provide NYSOC services. Recipient will bear the burden of proving any of the foregoing conditions exist.

ii. Notwithstanding the provisions of Section 11(a) herein and where written notice is provided to the Party disclosing the Confidential Information or Cyber Information, the Recipient 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 cyber security activities, provided that such third-party representative (1) is advised by the Party disclosing the Confidential Information or Cyber Information of the sensitive and confidential nature of such Confidential Information or Cyber Information; and (2) agrees to comply with the provisions of this IA as if they were a Party.

iii. 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 IA 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 IA;
   ii. Temporary Suspension of Obligations. At any time, a Party may suspend performance of one or more of its obligations under this IA 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 11(c)(ii) will not apply to Sections 11(a) and 16 of this IA.

12. NO THIRD-PARTY RIGHTS

Nothing in the IA 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 IA.

13. 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

Name:
Title:
Address:
Telephone Number:
Facsimile 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.

14. AMENDMENTS

This IA 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, or in the case of a waiver, the Party waiving compliance, and must be approved by the New York State Office of the State Comptroller if applicable.

15. 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 IA. 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.

16. 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 State 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 State or of its officers or employees when acting within the course and scope of their employment.

17. 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 IA.

18. ADDITIONAL REMEDIES

In addition to any other remedies available to the Parties under this IA 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 IA.

19. INDEPENDENT CONTRACTORS

Nothing in this IA shall be construed to create any partnership, joint venture or agency relationship of any kind. Neither Party has any authority under this IA 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.

20. ASSIGNMENT

The State may assign this IA, 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 IA 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 the New York State Office of the State Comptroller, if applicable.

21. 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 IA 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 IA shall constitute a waiver of any subsequent breach or breaches of such term.

22. ENFORCEABILITY/SECTION HEADINGS

In the event any clause, or any part or portion of any clause of this IA 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 IA 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 IA.

23. JURISDICTION

This IA 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 IA 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.

24. EXECUTION

By execution, delivery and performance of this IA, 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 IA constitutes the legal, valid, and binding obligation of the Parties hereto.

25. ENTIRE AGREEMENT

This IA 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.

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

By: The City of Oneida
.
Name: _____

Title: _____

Date: _____, 20___

NYS OFFICE OF INFORMATION TECHNOLOGY SERVICES

By: _____

Name: _____

Title: _____

Date _____ ,_20 _

NYS DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES

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

APPROVED AS TO FORM:	**APPROVED:**
NYS OFFICE OF THE ATTORNEY GENERAL	NYS OFFICE OF THE STATE COMPTROLLER
_____ By: _ Title: _ Date: __	_____ By: _ Title: _ Date: __

ATTACHMENT A
INTERGOVERNMENTAL AGREEMENT FOR THE PROVISION OF ENDPOINT PROTECTION AND RESPONSE SERVICES (Phase II)

BETWEEN

THE NEW YORK STATE OFFICE OF INFORMATION TECHNOLOGY SERVICES,

THE NEW YORK STATE DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES

AND

The City of Oneida

X052084

All Participating Entities will be provisioned with access to and training for the EDR software vendor's portal allowing the Participating Entity to perform monitoring, analysis, quarantine and containment, and other cyber hygiene functions as provided by the EDR software. In addition, the EDR software provides proactive threat hunting twenty-four hours per day, seven days per week (24x7). The EDR software will also be configured to conduct the first level of triage to identify threats, assign a level of importance or urgency to the threat, and deliver alerts and actionable notification directly to the Participating Entities thru E-mail.

A Participating Entity may choose additional levels of service from the NYSOC. These levels of service are either:

1. Off-hours monitoring, and email escalation; or

2. Off-hours monitoring, email escalation, critical escalations, and containment and/or quarantine actions on impacted endpoints flagged for such by the EDR software. By selecting this option, the Participating Entity is granting the NYSOC and/or the EDR software vendor's staff the authority to take action per the critical escalation process defined below.

Please indicate level of NYSOC service requested; if neither level of service is desired, enter N/A: _____.

Definitions:

Monitoring:
Monitoring is NYSOC and/or the EDR vendor staff reviewing Critical, High, and other vendor-escalated alerts received from the EDR software and conducting further analysis on the host endpoint using available tools (e.g., EDR Portal) to further quantify risk and determine if additional actions are required (e.g., escalation, critical escalation, containment and quarantine). The terms 'Critical' and 'High' alerts refer to the vendor's top two levels of automated alert criticality rating. 'Vendor-escalated' alerts refers to instances where the vendor escalates an alert to the NYSOC and/or Participating Entity beyond the vendor's automated alert criticality rating (e.g., Critical, High).

Escalations:
Escalation is the process of identifying potential cybersecurity concerns so that appropriate personnel can take action to address them. Escalations will be sent via email when the NYSOC Team and/or EDR software vendor's staff requires action to be taken by the Participating Entity in order to validate activity on a host or remediate a host. Examples of when an escalation will be sent may include, but would not be limited to:
- Validating questionable admin activity seen on a host
- Validating application usage
- Not having remote access to a host
- Requests for approval to take additional remediation countermeasures

Critical Escalations:
During an investigation, where NYSOC and/or EDR software vendor's staff containment and quarantine actions are required or action need to be taken by the Participating Entity, the NYSOC Team and/or EDR software vendor's staff will call the phone numbers provided in the below order of priority. If there is no response from any of the contacts, the NYSOC Team and/or EDR software vendor's staff will send a Critical Escalation email and continue monitoring but not proceed with any countermeasures that are not approved by the Participating Entity. The NYSOC and/or EDR software vendor's staff will begin the escalation process within a reasonable amount time from receipt of the critical alert or notification by the EDR software.

The Critical escalation and containment and quarantine functions will be phased in by the NYSOC and/or EDR software vendor's staff as it reaches operational maturity. Critical escalations may not be available on the Participating Entities' onboarding date. However, the EDR software will provide direct alerting to the Participating Entity irrespective of the NYSOC's status.

Containment and Quarantine:
NYSOC and/or EDR software vendor's staff containment and quarantine includes:
- Containment of hosts identified by the EDR software as a critical risk
- Quarantine or removal of files or artifacts identified by the EDR software as a critical risk
- Recommend recovery actions as needed per incident to address vulnerabilities in infrastructure not managed by the EDR software

Off-Hours: NYSOC Off hours support is Saturday and Sunday all day, and 5PM to 8AM Monday - Friday. The EDR software vendor's staff is available 24/7/365.

Escalation priority Points of Contact: Please provide a list **in order of priority** of the persons the NYSOC and/or EDR software vendor's staff should call when notifying the Participating Entity of a Critical Escalation (the Participating Entity does not have to use all the lines below and should add additional lines if necessary):

1. _____

2. _____

3. _____

4. _____

5. _____