MiCTA
Technology Solutions for Members Nationwide

verizon

MEMBER PARTICIPATION AGREEMENT

VERIZON BUSINESS NETWORK SERVICES INC.,	**STATE OF CONNECTICUT,**
on behalf of the Verizon affiliates identified herein ("Verizon")	**acting by its Department of Administrative Services ("Customer")**
22001 Loudoun County Pkwy.	**Attn.: Procurement**
Ashburn, VA 20147	**450 Columbus Avenue, Suite 1202**
	Hartford, CT 06103
	Member Number: _____
By: _	By: _
Nam	Nam
Title:	Title:
Date:	Date:

This Member Participation Agreement ("Agreement" or "PA") for Verizon Services, together with any attachments, schedules, and other documents made a part hereof ("Agreement"), is made by and between the above-named Customer and Verizon Business Network Services Inc., on behalf of MCI Communications Services, Inc. d/b/a Verizon Business Services and its affiliates and successors ("Verizon"). Verizon or its providing affiliate will provide to Customer the Services set forth herein. This Agreement is binding upon execution by both parties. The applicable rates, discounts, charges and credits, if any, shall be effective either: (a) when the Service is installed if Customer does not receive such Service prior to the execution of this Agreement; or (b) otherwise, on the first day of the second full billing cycle following execution and delivery of this Agreement by Customer to Verizon ("Effective Date").

WHEREAS Verizon and MiCTA, an association made up of non-profit colleges, universities, K-12 school systems, federal, state and local government units, health care providers, libraries and other non-profit entities, have entered into a Telecommunications and Internet Services Master Agreement ("Master Agreement"), based upon MiCTA's RFP MT TISA 2013 and Verizon's response thereto; and

WHEREAS, under the Master Agreement, Eligible Organizations who enter into a PA with Verizon may purchase from Verizon certain Services (identified in Attachment A to the Master Agreement) at the prices and/or discounts set forth in Attachment B to the Master Agreement; and

WHEREAS the Customer is an Eligible Organization and desires to purchase from Verizon certain Services available under the Master Agreement, and Verizon is willing to provide such Services on the terms and conditions set forth in this PA;

NOW THEREFORE, Verizon and Customer agree as follows:

GENERAL TERMS AND CONDITIONS

1. **Services**. Verizon will provide to Customer the services and products ("Services") identified in Attachment A to this Agreement.

2. **Term**. The "Term" of this Agreement shall begin on the Effective Date (defined above) and shall end on the last day of the twelfth (12th) month after the Effective Date (the "Initial Term"), at which time the Agreement will be automatically extended ("Extended Term") on a month-to-month basis until either party terminates it upon delivering sixty (60) days' prior written notice to the other party. The terms of this Agreement will continue to apply during any service-specific term commitment that extends beyond the Term stated above.

3. **Tariff and Guide**. Verizon's provision of Services to Customer will be governed by Verizon's international, interstate and state tariffs ("Tariff(s)") and by Verizon's "Service Publication and Price Guide" ("Guide"), as applicable and as supplemented by this Agreement. This Agreement incorporates by reference the terms of each Tariff and the Guide. The Guide is available to Customer on Verizon's Internet website (www.verizonbusiness.com/guide) ("Website"). Verizon may modify the Guide from time to time, and any modification will be binding upon Customer. Customer may sign-up for e-mail alerts of Guide changes. Except for new services, service features, service options or service promotions, which will become effective immediately upon their posting in the Guide on the Website, any modification made to the Guide will become effective on the date indicated in the Guide, provided that no such modification shall become effective and binding on Customer until it has been posted in the Guide for at least fifteen (15) calendar days. The contractual relationship between Verizon and Customer shall be governed by the following order of precedence: (i) the Tariffs to the extent applicable, (ii) the provisions of this Agreement, and (iii) the Guide.

4. **Changes to the Guide**. If Verizon makes any changes to the Guide that affect Customer in a material and adverse manner, Customer may discontinue the affected Service without liability by providing Verizon with written notice of discontinuance within sixty (60) days of the date such change is posted on the Website. Customer shall pay all charges incurred up to the time of Service discontinuance. Verizon may avoid Service discontinuance if, within sixty (60) days of receipt of Customer's written notice, it agrees to amend this Agreement to eliminate the applicability of the material and adverse change. A "material and adverse change" shall not include, nor be interpreted to include, (i) the introduction of a new service or any new service feature associated with an existing Service, including all terms, conditions and prices relating thereto, or (ii) the imposition of or changes to Governmental Charges (defined below). Notwithstanding any other provision in this Agreement, no material change may be made to the list of Services in Attachment A that alters the nature or scope of the Services or their intended use, with the exception of pricing for Services that are developed by a third party or contain third party service elements. Any replacement of a Service listed in Attachment A is conditioned upon the new service or services being of a similar nature and having a similar use as the replaced Service. An update of the Services through means other than changes to the Guide, or the addition of services that are related to or serve similar functions as the Services through means other than changes to the Guide, is permissible only with the prior written approval of Customer.

5. **Rates and Charges**. For the Services identified in Attachment A, Customer agrees to pay the rates and charges specified in Attachment B to the Master Agreement. Customer may not procure any service under this Agreement, unless the parties agree to incorporate such service into the Master Agreement. As used in this Agreement in connection with rates and charges, "standard" refers to rates and charges for Verizon Business Services III ("VBSIII") where applicable. Except where explicitly stated otherwise in the Master Agreement for a particular service, (a) all rates and charges are subject to change after the Initial Term, (b) all discount percentages set forth in the Master Agreement are fixed for the Term, (c) Customer will not be eligible to receive any other additional discounts, promotions and/or credits (Tariffed or otherwise), and (d) the rates and charges set forth in the Master Agreement do not include (without limitation) charges for all possible non-recurring charges, access service, local exchange service, charges imposed by a third party other than Verizon or a Verizon affiliate, on-site installation, Governmental Charges (defined below), network application fees, customer premises equipment or extended wiring to or at Customer premises. Verizon may give Customer notice of such changes in rates or charges by posting them on the Guide, by invoice message, or by other reasonable means (notwithstanding Section 19, Notices, below).

6. **Governmental Charges**. Verizon may recover amounts it is required or permitted by governmental or quasi-governmental authorities to collect from or pay to others in support of statutory or regulatory programs ("Governmental Charges"). Examples of such Governmental Charges include, but are not limited to, Federal Regulatory Fee, Primary Interexchange Carrier Charge cost recovery, and compensation payable to payphone service providers for use of their payphones to access Verizon's service.

7. **Taxes**. All rates and charges are exclusive of applicable taxes, tax-like charges, and tax-related charges, which Customer agrees to pay. If Customer provides Verizon with a duly-authorized exemption certificate, Verizon will exempt Customer in accordance with law, effective on the date Verizon receives the exemption certificate.

8. **Payment**. Customer agrees to pay all Verizon charges (except Disputed amounts, as defined below) within thirty (30) days of invoice date. The invoice date is the date the invoice is properly submitted. Payments must be made at the address designated on the invoice or other such place as Verizon may designate. Amounts not paid or Disputed on or before thirty (30) days from invoice date shall be considered past due, and Customer agrees to pay a late payment charge equal to the lesser of: (a) one and one-half percent (1.5%) per month, compounded, or (b) the maximum amount allowed by applicable law, as applied against the past due amounts. A "Disputed" amount is one for which Customer has given Verizon written notice, adequately supported by bona fide explanation and documentation. Any invoiced amount not Disputed within six (6) months of the invoice date shall be deemed to be correct and binding on Customer. Customer shall be liable for the payment of all fees and expenses, including attorney's fees, reasonably incurred by Verizon in collecting, or attempting to collect, any charges owed hereunder.

9. **Termination**. Either party may terminate this Agreement for Cause. As to payment of invoices, "Cause" means Customer's failure to pay any invoice (excluding Disputed amounts) within thirty (30) days after the invoice date, which failure has not been cured within ten (10) days of receiving notice of it. For all other matters, "Cause" means a breach by the other party of any material provision of this Agreement which has not been cured within thirty (30) days after delivery of notice.

10. **Disconnection of Service**. Customer shall provide prior written notice for the disconnection of Service, as follows. For Service provided exclusively within the United States, Customer must provide thirty (30) days written notice. For all other Service, Customer must provide written notice either (a) of sixty (60) days or (b) equal to the cancellation period required by third parties (such as PTTs) for the non-U.S. Mainland portion of the Service Customer is canceling, whichever is longer. Disconnection notices must be labeled conspicuously "Disconnect Request." Customer should contact its account representative or Customer Service if it does not receive confirmation of the disconnection from Verizon within five (5) business days. Notwithstanding any such termination, Customer will remain liable for any applicable early termination charges set forth in this Agreement.

11. **Confidential Information**. Commencing on the date Customer executes this Agreement and continuing for a period of three (3) years from the termination of this Agreement, each party shall protect as confidential, and shall not disclose to any third party, any Confidential Information received from the disclosing party or otherwise discovered by the receiving party while this Agreement is in effect, including, but not limited to, the pricing and terms of this Agreement, and any information relating to the disclosing party's technology, business affairs, and marketing or sales plans (collectively the "Confidential Information"). The parties shall use Confidential Information only for the purpose of this Agreement. The foregoing restrictions on use and disclosure of Confidential Information do not apply to information that: (a) is in the possession of the receiving party at the time of its disclosure and is not otherwise subject to obligations of confidentiality; (b) is or becomes publicly known, through no wrongful act or omission of the receiving party; (c) is received without restriction from a third party free to disclose it without obligation to the disclosing party; (d) is developed independently by the receiving party without reference to the Confidential Information, or (e) is required to be disclosed by law, regulation, or court or governmental order, including but not limited to any open records laws, freedom of information laws, or other "sunshine" laws to which Customer is subject.

12. **Disclaimer of Certain Damages**. NEITHER PARTY SHALL BE LIABLE TO THE OTHER FOR ANY INDIRECT, CONSEQUENTIAL, EXEMPLARY, SPECIAL, INCIDENTAL OR PUNITIVE DAMAGES, INCLUDING WITHOUT LIMITATION LOSS OF USE OR LOST BUSINESS, REVENUE, PROFITS, OR GOODWILL, ARISING IN CONNECTION WITH THIS AGREEMENT, UNDER ANY THEORY OF TORT, CONTRACT, INDEMNITY, WARRANTY, STRICT LIABILITY OR NEGLIGENCE, EVEN IF THE PARTY KNEW OR SHOULD HAVE KNOWN OF THE POSSIBILITY OF SUCH DAMAGES.

13. **Limitation of Liability**. THE TOTAL LIABILITY OF VERIZON TO CUSTOMER IN CONNECTION WITH THIS AGREEMENT, FOR ANY AND ALL CAUSES OF ACTIONS AND CLAIMS, INCLUDING, WITHOUT LIMITATION, BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, STRICT LIABILITY, MISREPRESENTATION AND OTHER TORTS, SHALL BE LIMITED TO THE LESSER OF: (A) DIRECT DAMAGES PROVEN BY CUSTOMER; OR (B) THE AMOUNT PAID BY CUSTOMER TO VERIZON UNDER THIS AGREEMENT FOR THE SIX (6) MONTH PERIOD PRIOR TO ACCRUAL OF THE MOST RECENT CAUSE OF ACTION. NOTHING IN THIS SECTION SHALL LIMIT VERIZON'S LIABILITY: (A) IN TORT FOR ITS WILLFUL OR INTENTIONAL MISCONDUCT; OR (B) FOR BODILY INJURY OR DEATH PROXIMATELY CAUSED BY VERIZON'S NEGLIGENCE; OR (C) LOSS OR DAMAGE TO REAL PROPERTY OR TANGIBLE PERSONAL PROPERTY PROXIMATELY CAUSED BY VERIZON'S NEGLIGENCE.

14. **Assignment**. Either party may assign this Agreement or any of its rights hereunder to an affiliate or successor without the prior written consent of the other party, provided that if Customer assigns this Agreement to an affiliate or successor, then such affiliate or successor must meet Verizon's creditworthiness standards. Any attempted transfer or assignment of this Agreement by either party not in accordance with the terms of this Section shall be null and void.

15. **Service Marks, Trademarks and Name**. Neither Verizon nor Customer shall: (a) use any service mark or trademark of the other party; or (b) refer to the other party in connection with any advertising, promotion, press release or publication unless it obtains the other party's prior written approval.

16. **Governing Law; Disputes**. Except as the Parties may otherwise expressly agree, this Agreement shall be governed by the laws of the state where the Services are provided by Verizon to Customer's locations. Any litigation arising out of or in connection with this Agreement may be brought for trial in any Federal or state court of competent jurisdiction. The parties agree that any such trial shall be without jury. Non-U.S. Services shall be subject to applicable local laws and regulations in any countries where such Services originate or terminate, including applicable locally filed Tariffs. Customer acknowledges that Verizon is governed by the Communications Act of 1934, as amended, and as interpreted and applied by the Federal Communications Commission.

17. **Notice**. All notices, requests, or other communications (excluding invoices) hereunder shall be in writing and either transmitted via overnight courier, electronic mail, hand delivery or certified or registered mail, postage prepaid and return receipt requested to the parties at the following addresses. Except as otherwise provided, notices will be deemed to have been given when received. Customer's notice address is provided on Page 1 of this Agreement unless otherwise noted.

To Verizon:
Verizon Enterprise Services
22001 Loudoun County Parkway, F2-2-278
Ashburn, VA 20147
Attn: Richard Trenz, Managing Client Partner, Public Sector.
Tel: 703-886-3723
Email: richard.trenz@verizon.com

and to:
Verizon Enterprise Services
22001 Loudoun County Parkway, F2-2-115
Ashburn, VA 20147
Attn: Margaret Hallbach

With fax copies to:
Verizon Business Services
22001 Loudoun County Pkwy
Ashburn, VA 20147
Attn: Vice President, Legal
Fax: 703-886-5807

18. **Acceptable Use**. Use of Verizon's Internet Service(s) and related equipment and facilities must comply with the then-current version of the Verizon Acceptable Use Policy ("Policy") for the countries from which Customer uses them (see www.verizonbusiness.com/terms). Customer shall be liable to Verizon for any losses, damages, claims, costs or expenses sustained or incurred by Verizon resulting from any violation by Customer of the Policy. Each party will promptly notify the other of any such claim.

19. **Domain Names**. Customer shall ensure that its use of any domain name registered or administered on Customer's behalf does not violate the service mark, trademark or other intellectual property rights of any third party. Any violation of this Section is deemed a material breach establishing Cause for termination. Verizon shall have no liability for any claims that may arise from the acts or omissions of domain name registries, registrars or other authorities.

20. **Resellers/Subcontractors.** Verizon agrees to assume ultimate responsibility in all aspects for the performance of all reseller/ subcontractors, if any, utilized to provide products and/or services to Customer under this Agreement. Verizon takes the overall responsibility and acts as the single point of contact for services purchased from Verizon under this Agreement including, but not limited to, the following:

    20.1 Addressing all service and product issues, and providing Customer favorable resolution to any reported problems;

    20.2 Processing and tracking all Customer purchase orders placed through resellers/subcontractors;

    20.3 Responding to any/all issues related to delivery, installation, warranty, support, etc. when services and/or products were processed through a reseller / subcontractor; and

20.4 Acting as the primary liaison between reseller/subcontractor and/or manufacturer on behalf of the Customer.

21. **Appropriated Funding.** If (a) the Term of this Agreement is greater than one (1) year and (b) Customer is purchasing services hereunder solely with funds that are legislatively-appropriated on a single fiscal year basis and Customer is therefore required by applicable law to reserve the following right in all multi-year purchase contracts, then Customer reserves the right to cancel this Agreement, upon not less than thirty (30) days' notice, whenever such funds have failed appropriation or are otherwise made unavailable to Customer to support continuation or performance in any fiscal year succeeding the first.

22. **Compliance with Law.** Verizon (including its subcontractors, if any) and Customer, shall each at their own expense operate in full compliance with all applicable Federal, State and local laws, rules and regulations. Verizon shall maintain in force all licenses and permits required by the states in which it conducts business.

23. **Financial Stability.** Verizon acknowledges that Customer may rely on Verizon's annual and quarterly financial statements and any required Securities and Exchange Commission Certification Reports as a measure of Verizon's financial strength and ability as an ongoing business concern to fulfill its obligations under this Agreement.

24. **Service Level Agreement (SLA).** Unless Customer and Verizon otherwise expressly agree in writing, Verizon's standard SLAs, if any, for the services/products provided under this Agreement shall apply. Should Customer desire other SLAs to meet their specific organizational requirements, Verizon and Customer may negotiate such SLAs, including: services, features, hardware and/or software to be covered; measurable standards of performance and/or quality of service; Customer/Verizon responsibilities defined; Customer's recourse for system and/or hardware/software failure to meet the SLA; and any other element that is mutually agreed upon by both parties, including any cost adjustments for negotiated SLAs. Any negotiated SLAs shall be made part of this Agreement.

25. **Force Majeure.** Neither party shall be liable for any delay or failure in the performance or provision of Services under this Agreement arising out of acts or events beyond its reasonable control, including but not limited to acts of God, war, terrorist acts, fire, flood, catastrophe, severe weather, cut cable, explosion, riot, embargo, acts of the Government or third parties, labor disputes or strikes, or unavailability of necessary facilities or equipment.

26. **Entire Agreement.** This Agreement (and any Attachments and other documents incorporated herein by reference) constitutes the entire agreement between the parties with respect to the Services ordered under this Agreement and supersedes all other representations, understandings or agreements that are not expressed herein, whether oral or written. Except as otherwise set forth herein, no amendment to this Agreement shall be valid unless in writing and signed by both parties. Any requirement for a signature in this Agreement or any Amendment may be satisfied by facsimile transmission of an original signature. Any terms, conditions, or other contents of any purchase order or similar document issued by Customer shall not apply in any way to add to, delete, or modify the terms and conditions of this Agreement, and shall be deemed to be issued only for administrative purposes to reflect Customer's order for the products or services listed herein under the terms of this Agreement.

ATTACHMENT A
to Member Participation Agreement

Customer name: State of Connecticut

1. **Service.** The Services that Customer may order under this Member Participation Agreement ("Agreement") are those set forth in the MiCTA Master Agreement, including but not limited to the Services set forth below. The rates and charges that shall apply to such Services are the rates and charges that apply under the terms of the MiCTA Master Agreement, including Attachment B of said Master Agreement, which are incorporated herein and made a part of this Agreement.

2. **Services Ordered.** The parties acknowledge for informational purposes that the Customer's initial order for Services under this Agreement shall consist of the following. Any additions or changes to the following may be made pursuant to the terms of this Agreement.

MiCTA Schedule 9.4.4m - Managed Security Services - Analytics

Service	Price
Non-Recurring Charges	
Site Set-up fee (CK)	$2,500
Set-up per site	$1,000
Total NRC	**$3,500**
Monthly Recurring Charges	
MSS-Analytics, Daily Ingest Data Volume Tier, 100-200 GB/day data ingest	$34,000
Security Lifecycle Engineer (SLCE) -10 hours per week	$ 6,800
Total MRC	**$40,800**

Note: In the event of a discrepancy between the rates and charges set forth above and the rates and charges applicable pursuant to the MiCTA Master Agreement, the rates and charges applicable pursuant to the MiCTA Master Agreement shall apply.

2.1 Term Commitment. Customer shall purchase the above Services for a minimum period of 12 consecutive months (the "Initial Term") following the execution of this Agreement and installation of the Service.

2.2 Service Locations. The above Services shall be provided to Customer under this Agreement at the following locations.

55 Farmington Avenue, Hartford, CT 06105

Other Customer locations may be added to this Agreement, or changed, only upon mutual assent of the parties.

3. **Service Attachment.** Service Attachment(s) for the above Services, if applicable, that are attached hereto or set forth in the MiCTA Master Agreement or Guide, are incorporated herein by reference and shall be a part of this Attachment A. The following documents are attached to this Attachment A:

Exhibit 1: Schedule 9.4.4m (Managed Security Services—Analytics Service Attachment

Exhibit 2: Statement of Work—Client Security Engineering Analyst

EXHIBIT 1
TO ATTACHMENT A OF
MEMBER PARTICIPATION AGREEEMENT

Routing Code: 8

Schedule 9.4.4m
Managed Security Services – Analytics
Service Attachment

Part I: Rates and Charges

1. **Rates and Charges for United States Contracts.** Customer will pay the non-recurring charges ("NRCs") and monthly recurring charges ("MRCs") per MSS – Analytics service and per the daily ingest data volume tier (or per other specified item) as set forth below. The NRC is billable for new installs or physical location moves. Unless expressly indicated otherwise, all NRCs will be invoiced upon Order Confirmation Date and the initial MRCs will be invoiced upon RFS.

1.1 Non Recurring Charges.

MSS – Analytics	Setup NRC
A-Site set-up fee (CK)	$2500
A-Site set-up fee (CK) HA	$5000
A-Hosted Local Event Collector (per Customer)	$500
A-Hosted Local Event Collector HA (per Customer)	$500
A-Remote set up of Connection Kits, terminal servers and modems for Customer-owned equipment.	$500
A-High Availability Configuration: Remote set up of Connection Kits, terminal servers and modems for Customer-owned equipment.	$1000
A-Set-up per site - single Serviced Device	$1000
A-Set-up per site (HA) - single Serviced Device	$2000
A-Package of 12 Service Tickets	$600
A-Move CK	$500

1.2 Monthly Recurring Charges.

1.2.1 MSS –Analytics.

Daily Ingest Data Volume Tier	MRC
0-10 GB/day data ingest	$7400
10-50 GB/day data ingest	$13000
50-100 GB/day data ingest	$20000
100-200 GB/day data ingest	$34000
200-500 GB/day data ingest	$45000

1.2.2 Client Security Life Cycle Engineer

Service Tier	MRC
Dedicated SLCE-40 hours per week	$24,000.00
Dedicated SLCE-30 hours per week	$18,300.00
Dedicated SLCE-20 hours per week	$12,525.00

Dedicated SLCE-10 hours per week	$ 6,800.00

1.3 **Discounts.**

1.3.1 **Term Discount.** A term discount will be applied to the MSS – Analytics service MRC charges specified in Monthly Recurring Charges clauses above as outlined in the table below. Such term discount is based upon the stated term of the master agreement that governs the relationship between Customer and Verizon (the "Agreement") or the term of the Contract for MSS –Analytics, as applicable.

Agreement Term	Discount
1 Year	0%
2 Year	10%
3+ Year	15%

1.3.2 **Term or Volume Discount Shortfall.** In the event Verizon grants Customer term and such Initial Order Commitment is not met or Term is not completed as a result of Customer's termination of one or more MSS – Analytics service for convenience or Verizon's termination of one or more MSS – Analytics service for Cause; then the MRCs and NRCs payable will be adjusted in accordance with the discount, if any, Customer would be eligible to receive based on the actual business Initial Order Commitment or Term achieved and Customer shall pay such additional amounts as may become due as a result of such adjustment.

2. **Rates, Charges and Discounts for Non-US Contracts.**

2.1 **Rates and Charges.** Non-recurring charges ("NRCs") are billable for new installs or physical location moves. Unless the parties agree otherwise in writing, all NRCs will be invoiced upon the Order Confirmation Date and the initial MRC will be invoiced upon RFS.

2.2 **Discounts.** Discounts, if any, will be automatically applied to each Service Order, depending on the term of the Agreement indicated in the Service Order.

Part II: Service Description and Requirements

Description of Service. MSS - Analytics provides 24x7x365 analysis of Customer-supplied data for the purpose of monitoring, detecting and alerting Customer to potential security threats, Security Events and Security Incidents. The service uses an advanced, analytics-based approach capable of monitoring any device that generates data, not just traditional security and network devices. In addition to detecting traditional signature-based threats, MSS – Analytics uses behavioral modeling to detect advanced threats and provide valuable insights that can help shorten the detection interval. Verizon's global SOCs are staffed with security analysts who monitor and escalate threats as the analytics platform collects and analyzes data.

Capitalized terms used in this Service Attachment have the meaning ascribed to them in Part V (Definitions) of this Service Attachment. Due to the inherent evolutionary nature of technology, Verizon reserves the right to change, modify, update or enhance MSS – Analytics Service Description from time to time. The Service Description provides additional details and information regarding service settings and service delivery. Verizon will notify Customer upon publishing a new release of the Service Description by (a) posting the updated Service Description to the Security Dashboard or (b) communication via the SSA. New releases of the Service Description are effective upon such release.

1.1 **Implementation of MSS - Analytics**. Prior to commencement of MSS –Analytics , Verizon will schedule a kick off meeting to introduce the Verizon service delivery team, identify the appropriate contacts for Customer, discuss the scope of the MSS – Analytics service and its business impacts, and obtain any required information from Customer. Upon receipt from Customer of a completed deployment kit, Verizon will create a proposed project plan with high-level milestones and timelines. Verizon will only provision MSS - Analytics after Customer has approved the project plan. During the implementation of MSS - Analytics, Customer may propose changes to the project plan. Verizon will assess Customer's proposal and may require Customer to submit a new Service Order or execute an Amendment to this Service Attachment to memorialize the approved changes.

1.1.1 **Customer Responsibilities.** Customer must complete a deployment kit and provide such deployment kit to Verizon within 15 Business Days of the kick off meeting or Verizon may terminate

Customer's order for MSS - Analytics. If Customer fails to approve the project plan, or fails to provide any necessary information to implement the project plan, and such delay causes any activity on the critical path of the project plan to be delayed by more than 25 Business Days, Verizon may terminate Customer's order for MSS - Analytics. Upon termination of an order for MSS - Analytics service, Verizon may charge Customer for any expenses incurred by Verizon (including labor fees) through the date of termination.

1.2 **Threat Analysis.**

1.2.1 **Overview.** MSS – Analytics analyzes data received from Data Sources to identify possible Security Incidents and potential indicators of compromise. A Security Incident is generated after data have been processed, or analyzed, against Security Content on Verizon's security analytics platform. MSS – Analytics both (a) analyzes individual pieces of data and events which may, individually, appear to be harmless and (b) correlates those events and data with other data to determine if a more harmful pattern presents itself, thus identifying a Security Incident.

Types of data used in Incident correlation can include:

- Any and all data provided by Customer
- Information in the Service Context, such as the classification of an asset
- Verizon's Threat Intelligence

1.2.2 **Security Incident Classification**

Verizon Classifies Security Incidents into 4 Categories:

Incident Classification	Risk Levels	Conditions
Insufficient Info	L0	The Incident has been classified as 'Insufficient Info' based on the associated events.
Harmful Attack	L1	The Incident is identified as an attack or an attempted attack that may result in damage or unauthorized access to a device or application. The cause of the Incident renders Customer's infrastructure vulnerable or compromised.
Harmless Attack	L2	The Incident is identified as a known attack, attempted known attack or reconnaissance effort. Customer's infrastructure is not considered vulnerable or compromised based on the Service Context.
False Positive	L4	The Incident may be falsely triggered, is informational or benign in nature.

Offline Analysis Category is used during first phase of deployment

Classification	Level	Conditions
Offline analysis	L 9	Level is used during the first phase of deployment or after major changes in the network (such as adding or removing a server or Serviced Device, moving a Serviced Device, changing security policies and rule sets, installing major signature updates or major software upgrades, implementing an Urgent Change Request or replacing a Serviced Device. These Events will only be logged and will not involve real-time analysis.

1.2.3 **Security Incident Handling**. Verizon will generate Security Incidents in both real- and non-real time, depending on the detection method. The status of the Incident will be changed throughout its lifecycle. Status changes are communicated by Email and are displayed on the Security Dashboard. An SMC Time Stamp ("UTC") is added after each 'status' change. A Security Incident can have the following status:

Security Incident Status

Incident Status	Conditions
Open (Security Incident Detection)	The Incident has been generated based on Verizon's threat detection policies.
Escalated (Security Incident handling)	An Incident Record Communication is created with the Security Incident information to allow the mitigation, containment or resolution of the risk. A Security Incident is escalated when it is: o A Harmful Attack Incident and concerns a real threat o An Insufficient Info Incident: the security analyst needs extra information to classify the Security Incident
Closed	The Incident has been auto-closed or closed by the security analyst.

An Incident classification and status may change based on additional analysis, intelligence information or after Customer feedback has been received

1.2.3.1 **Real-Time Security Incidents.** Verizon uses threat detection policies based on one or more use cases to create Security Incidents in real time. All use cases and proprietary signatures are categorized to help (a) increase insight into Security Incidents and (b) reduce the number of false-positive Incidents. The Incident descriptions provide recommendations on possible actions Customer can take.

1.2.3.2 **Non-Real Time Security Incidents.** Verizon uses threat detection policies based on one or more use cases in order to find patterns in data collected over a longer period of time and to allow low confidence indicators to be analyzed more effectively. Security analysts will review these Incidents periodically as a block of security information. If an Incident or a combination of Incidents is considered to be important, the SOC will escalate it. This method optimizes Security Incident handling and focuses on escalating potentially harmful Incidents and reducing Insufficient Info Incidents and False Positives. The Security Incident Escalation SLA does not apply for non-real time security incident handling.

1.2.4 **Security Incident Escalation.** Verizon will only escalate Security Incidents that are classified as 'Insufficient Info' and 'Harmful Attack.' Verizon will examine the characteristics and context of the events and Incidents, and evaluate the possible impact of a threat/attack before escalating an Incident Record Communication. Verizon will provide additional information to support the investigation of a Security Incident and may propose possible recommendations for next actions. Verizon will not provide remediation services.

Customer:

- Must provide missing Incident information for Incidents classified as 'Insufficient Info' within the required timeframe; if Customer fails to provide such information, Verizon may send a reminder or change the status of the Incident to 'Closed.'
- Must inform Verizon of any remediation actions Customer has taken in order to enable Verizon to update its inventory of Customer's infrastructure and set the Incident status to 'Closed.'

Verizon will Escalate an Incident Record Communication with the Following Incident Information:

- UTC timestamp of the Incident creation
- Source information and destination information
- Threat Signature and use case information, if applicable: threat use case ID, name, and description
- Packet dumps, if obtainable from the Data Source using the existing infrastructure.

Targets for Security Incident Escalation

	Communication	Communication	Reporting
Channel	Email	Phone and Email	Security Dashboard
Information Type	Incident Record Communication - Insufficient Info (L0)	Incident Record Communication - Harmful Attack (L1)	Security Dashboard
Reference Time	SMC Time Stamp (UTC) Incident Creation	SMC Time Stamp (UTC) Incident Creation	
Response Time	≤ 30 minutes after Incident Creation	≤ 15 minutes after Incident Creation	Refreshed every 15 minutes
Contact Person	Authorized Contacts	Authorized Contacts	Authorized Contacts

There are no service level targets for Incidents created in non-real time.

1.2.5 **Service Management and Reporting.**

1.2.5.1 **Security Dashboard** Authorized Contacts have 24x7 access to the Security Dashboard. Each Authorized Contact must have one SSL Certificate to access the Security Dashboard. MSS – Analytics includes provision of up to five SSL Certificates. The set-up of an additional Authorized User, and associated SSL Certificate, uses two Service Tickets.

1.2.5.2 **Request for Information.** Customer may submit a RFI through the Security Dashboard. Customer will receive a unique call ID that must be used in all further communications on this RFI. Each question uses one Service Ticket. No Service Tickets will be charged if the RFI is related to an existing escalation of an 'Incident', 'Health' or 'Other' Incident. Service Tickets are charged once a Serviced Device has been declared Ready for Operations ("RFO"). Inquiries not directly available through the Security Dashboard, or which require a more detailed analysis compared to what is available in the Incident Reports, will not be considered as a regular RFI. Examples of such requests are requests to retrieve raw data for forensics and additional one-time reports. Verizon may accept such requests pursuant to a separate written agreement and charged at the Applicable Rates.

1.2.5.3 **Data Availability and Retention.** Incidents are stored in a Verizon proprietary format in the SMC database for one year, unless otherwise mutually agreed by the parties in writing. Archived incidents requested by the Customer will be made available in Comma Separated Value (CSV) format or another format mutually agreed upon by the parties.

Verizon will store raw data associated with Events for one year. Raw data associated with Events linked to a Data Source that occurred during the immediately preceding one- year period will be made available upon Customer's request up to one month after service has ended with respect to such Data Source. At the end of the retention period, logs and Customer data will be disposed of according to the relevant Verizon Asset Classification and Handling Policy.

Data can be retrieved via a RFI ticket through the Security Dashboard and will be provided either as a downloadable file on the Security Dashboard or via an appropriate storage medium. The response time is dependent on the amount of data to be retrieved and the complexity of the request.

In order to enable the most comprehensive analytics capabilities customer-provided device data is enriched with additional Verizon-provided metadata such as Timestamps, DNS lookup of internal and external IP addresses, reputation score of external IP addresses, etc. as appropriate to the specific customer-supplied data source.

1.2.6 **Change Requests.**

1.2.6.1 **Customer-Initiated Change Requests.** Customer-Initiated Change Requests may only be submitted by Authorized Contacts through the Security Dashboard. Verizon may reject Change Requests that are not properly submitted (e.g., a Change Request not submitted on the Security Dashboard or an ambiguous or unclear Change Request). Verizon will notify the Authorized Contact via Email if a Change Request is rejected.

Verizon will assign a unique number to each Change Request submitted. Customer must use this number in all communications about the Change Request. Service Tickets may be required for Change Requests. The number of Service Tickets consumed for an implemented Change Request is determined by the type of Change Request and SLA Verizon requires to accept and implement the Change Request. Verizon may ask Customer for additional confirmation and authorization before implementing a Change Request. In this event, Verizon will send a confirmation request to the Authorized Contacts. A Change Request has a status in each phase of its lifecycle as shown below. When the status changes, Verizon will attach an SMC Time Stamp and notify Customer via Email. The Managed Security Services Change Management Overview document provides details and conditions regarding the different types of Customer-initiated Change Requests, as described below.

Status Levels in the Acceptance Phase	**Change Request Conditions**
New	The Change Request has been received by Verizon.
Assigned	The Change Request has been assigned to a Security Analyst.
Reopened	The Change Request has been reopened for further action or feedback. This may be due to an internal Customer or failed change.
Work in Progress	The Change Request is being managed by a Security Engineer.
Hold	The Change Request is under review and the SLA is paused.
Status Levels in the Implementation Phase	**Change Request Conditions**
Hold - Accepted	The Change Request has been reviewed and accepted for implementation. The implementation SLA is in effect.
Hold - Internal	The Change Request has been put on hold by Verizon and the implementation SLA is in effect.
Hold – Under Review or Pending Peer Review	The Change Request is pending an action from Verizon. The implementation SLA is in effect.
Hold – Customer Request or Awaiting Customer Feedback	The Change Request is on hold by request from Customer or it is on hold pending an action by Customer which is preventing the implementation of the Change Request. The implementation SLA is not in effect.
Hold – Internal Vendor	The Change Request is pending an action by a Verizon vendor and implementation of the Change Request is pending. The implementation SLA is in effect.
Hold – Customer's Vendor	The Change Request is pending an action by Customer's vendor, which is preventing the implementation of the Change Request. The implementation SLA is not in effect, as Verizon is awaiting the action from Customer's vendor.
Hold – Scheduled Work	The Change Request has been scheduled for a specific date and time to activate the Change Request. The implementation SLA is in effect.
Status Levels in the Verification Phase	**Change Request Conditions**
Resolved - Discarded	The Change Request has been discarded. The implementation SLA is stopped.
Resolved - Implemented	The Change Request has been implemented. The implementation SLA is stopped.

Closed	The Change Request has been implemented and Customer has verified the implementation. No further action is required.

1.2.6.2 **Regular Change Request.** Verizon will review and accept a Regular Change Request ("RCR") within 24 hours after submission. Verizon will implement an accepted RCR in the next Maintenance Window, provided that the minimum time between Customer's submission of a RCR and Verizon's implementation of such request will be 48 hours. RCRs consume 2 Service Tickets.

1.2.6.3 **Major Change Request.** A Major Change Request may be needed in addition to a RCR. Such a change can be implemented subject to a separate written agreement and charged at the Applicable Rates. There are no SLAs for the implementation of a 'Major Change Request.' Verizon can implement such a change (a) subject to a separate written agreement and charged at the Applicable Rates or (b) charged at a mutually agreed upon number of Service Tickets.

1.2.6.4 **Verizon-Initiated Emergency Change Request.** Verizon may implement emergency Change Requests, such as disabling Threat Signatures under the following circumstances:

- Verizon witnesses or is notified of a massive attack of a virus/worm outbreak that poses a risk of flooding Verizon's infrastructure.

Verizon is authorized to disable Threat Signatures in emergencies according to the notification timeline for an Urgent Change Request.

1.2.7 **Security Services Advisor.** Customer is assigned a SSA, who will host a quarterly service review meeting. The SSA is assigned to multiple MSS – Analytics customer accounts and is not dedicated to Customer. The SSA:

- Provides training on the Security Dashboard
- Manages Customer Communication and Security Advisories
- Manages service issues and Service Credit requests

Part III: Service Terms and Conditions

1. **Maximum Daily Data Ingest Volume.** Customer must commit to a Maximum Daily Data Ingest Volume. Verizon will monitor Customer's Daily Data Ingest Volume and post a monthly Data Ingest Volume report to the Security Dashboard.

   If Customer's Daily Data Ingest Volume exceeds Customer's committed Maximum Daily Data Ingest Volume by more than 10% in 2 consecutive months, Verizon will notify the Authorized Contacts by Email. Customer will have 30 days after Verizon's notice to reduce its Daily Data Ingest Volume in order to remain within the committed Maximum Daily Data Ingest Volume. If Customer fails to reduce its Daily Data Ingest Volume within such 30-day period, Customer will automatically be moved into the next higher Daily Data Ingest tier.

Daily Data Ingest Tier:
100-200 GB/day

1.1 **Excluded Services.** The parties acknowledge that Verizon has no obligation to provide MSS – Analytics for any Data Source that: (i) runs a version of operating system and/or application software that is not supported by Verizon, or that is no longer supported or maintained by the relevant manufacturer or licensor; or (ii) has not been properly registered and/or for which required permits or approvals are not or no longer maintained.

2. **Customer Responsibilities.**

2.1 **Asset Criticality Data.** Customer acknowledges that, without up-to-date asset criticality data, Verizon's ability to classify potential threats and Incidents accurately will be limited, resulting in the increased possibility of false-positives and inaccurate impact assessments.

2.2 **Maintenance Contracts.** Customer will (a) at its own expense, procure and maintain with each vendor adequate maintenance contracts and all licenses necessary for the Data Sources to enable Verizon to properly perform MSS –Analytics; (b) comply with MSS - Analytics prerequisites and operational procedures as set forth in the applicable terms; and (c) promptly inform Verizon of any changes in Customer's Environment and any changes to the nomination and/or authorization level of the Authorized Contacts to oversee, monitor or evaluate the provision of MSS -Analytics.

2.3 **Interoperability.** Customer acknowledges that modifications or changes to the Data Sources (such as future releases to the Data Source's operating software) or to the Customer Environment may cause interoperability problems, inability to transmit data to Verizon or malfunctions in a Data Source and/or the Customer Environment. Customer will give Verizon written notice (notice via email is acceptable) of any modifications or changes within 5 Business Days after making any such changes. Customer acknowledges that it is Customer's responsibility to maintain, at its sole cost and expense, the Customer Environment to ensure that the Customer Environment is interoperable with each Data Source.

2.4 **Minimum Orders.** Customer acknowledges and accepts that some MSS - Analytics services may require a minimum order quantity. Verizon will advise Customer if a minimum order quantity applies in advance of Customer's order. Any unused portion of such minimum quantity will be forfeited upon termination or expiration of the related MSS - Analytics service and Customer will not be entitled to receive any refund, credit or other form of reimbursement of fees paid in respect of such unused portion.

2.5 **Service Equipment.** Verizon may use Service Equipment to collect Logs and Events from Data Sources and to forward such Logs and Events to the SMC (e.g., Connection Kits). If Verizon determines that a Service Equipment is needed on Customer's Site, Customer must either: (a) provide such Service Equipment subject to Verizon's specifications, or (b) Verizon may provide Service Equipment to a limited number of countries for an additional charge. Verizon will configure and access such equipment remotely. Where Verizon supplies Service Equipment, Customer will return such Service Equipment at Customer's sole cost to the address indicated by Verizon upon termination of MSS - Analytics. Service Equipment must be returned in the same condition as they were originally delivered, normal wear and tear excepted, and packaged in the original packaging or other equivalent packaging materials. If Customer fails to return the Service Equipment within 14 days following the termination of MSS - Analytics, Customer will pay the greater of: (a) 50% of the relevant per site set-up NRC indicated in the Service Attachment/Service Order, or (b) the actual cost and expense to replace such Service Equipment.

2.6 **User Interface.** In connection with the provision of MSS – Analytics, Verizon may provide Customer with one or more user Logins to access a User Interface. The User Interface and Login may be used for accessing on-line services or authorizing instructions and requests.. Customer will at all times keep its Login strictly confidential and will take all reasonable precautions to prevent unauthorized use, misuse or compromise of its Login. Customer agrees to notify Verizon promptly upon learning of any actual or threatened unauthorized use, misuse, or compromise of its Login. Verizon is entitled to rely on Customer's Login as conclusive evidence of identity and authority. Customer will be liable for all activities and charges incurred through the use of Customer's Login, and will indemnify, defend and hold Verizon harmless from all liabilities, losses, damages, costs and expenses (including, without limitation, reasonable attorneys' fees and costs) incurred by Verizon to the extent resulting from the use and/or compromise of Customer's Login, unless the unauthorized use, misuse or compromise of Customer's Login is solely attributable to Verizon's gross negligence or willful misconduct.

2.7 **Installation Sites and Equipment.** Customer will prepare any installation site in accordance with Verizon's instructions to ensure that any equipment that interfaces with Customer's computer system is properly configured as required for the provision of MSS - Analytics and operates in accordance with the manufacturer's specifications. All Data Sources must have a routable network path to the Service Equipment and, if required, an agent must be loaded on each Data Source. Customer will install and maintain software agents required for the provision of MSS - Analytics to Data Sources (e.g., for syslog logging for operating system and active directory server), at its cost. If Customer fails to make any preparations required herein and this failure causes Verizon to incur costs during the implementation or provision of MSS - Analytics, then Customer agrees to reimburse Verizon promptly for these costs.

2.8 Customer acknowledges and agrees that MSS - Analytics is offered and provided by Verizon to multiple customers doing business in various industries. Absent terms to the contrary in the Agreement, MSS - Analytics is implemented without specific controls that may generally be required or customary for customers in any particular industry and is not designed to satisfy any specific legal obligations. Customer shall be solely responsible for determining that MSS - Analytics satisfies Customer's obligations under law or contract. Customer agrees to use MSS - Analytics in accordance with all applicable laws and not to use MSS - Analytics in any manner that imposes obligations on Verizon under any laws other than those laws with which Verizon agrees to comply as specifically set forth in the Agreement. Without limiting the generality of the foregoing, Customer agrees not to cause, or otherwise request that Verizon create, receive, maintain or transmit protected health information (as defined at 45 C.F.R. § 160.103) for or on behalf of Customer in connection with MSS - Analytics or in any manner that would make Verizon a business associate (as defined at 45 C.F.R. § 160.103) to Customer. In the event Customer acts or uses MSS - Analytics in a manner not permitted under this Section 2.8, Customer shall (a) be in material breach of the Agreement, including this Service Attachment; (b) indemnify, defend and hold harmless Verizon for any losses, expenses, costs, liabilities, damages, penalties, investigations or enforcement proceedings (including attorneys' fees) arising from or relating to Customer's breach of this Section 2.8; (c) take, at Customer's expense, prompt action to correct and/or mitigate the effects of Customer's breach of this Section 2.8; and (d) provide Verizon with reasonable cooperation and support in connection with Verizon's

response to Customer's breach of this Section 2.8. Customer shall assume and be solely responsible for any reporting requirements under law or contract arising from Customer's breach of this Section 2.8.

3. **Warranties.**

3.1 **Verizon Warranties.** Verizon warrants to Customer that it will perform its obligations in a good and workmanlike manner. The remedies set forth in Part V (Service Level Agreement) are Customer's sole and exclusive remedies in connection with the portions of MSS - Analytics related to the failure to meet any standard set forth in the SLA. Verizon does not warrant that MSS - Analytics will detect and prevent all possible threats and vulnerabilities or that such services will render Customer's network and systems invulnerable to all security breaches and vulnerabilities.

3.2 **Customer Warranties.** Customer represents and warrants that (a) it has and will continue to have all rights, power, permissions and authority necessary to have Verizon perform MSS - Analytics in the Customer Environment (including, without limitation, all rights, power, permissions and authority necessary in respect of any IP address assigned to a Data Source, including consent of all authorized network users) and (b) consents to Verizon's performance of MSS – Analytics. Customer hereby assumes the sole responsibility for the accuracy of the IP addresses and domains provided to Verizon. Customer will be liable for all costs and expenses from any third party claims of loss, damage (including reasonable attorneys' fees) and liability of any kind that may be incurred as a result of Customer's breach of the foregoing warranty.

3.3 **Third Party Warranties.** For any third party products and/or services incorporated as part of MSS - Analytics, Customer will receive only the warranties offered by such third party to the extent Verizon may pass through such warranties to Customer.

4. **Termination.**

4.1 **Renewal.** Each order will renew for a Term of 1 year, unless either party provides written notice at least sixty (60) days prior to the expiration of the then-current Term.

4.2 **Pre-RFS Termination**. Either party may terminate a request for MSS - Analytics MSS - Analytics service for any Serviced Device prior to RFS with or without Cause, effective thirty (30) days after written notice of cancellation. If Customer requests termination of an MSS - Analytics MSS - Analytics service prior to RFS as set forth under this provision, or Verizon terminates an MSS - Analytics service as a result of Customer's failure to provide the necessary information or reasonable assistance required by Verizon to provision MSS - Analytics service, Customer will pay any set-up fees and other amounts accrued for MSS - Analytics through the date of such termination plus an amount equal to any applicable annual third party license fee. Customer will pay the invoice for such charges in accordance with the terms of the Agreement.

4.3 **Post-RFS Termination.** Either party may terminate any MSS - Analytics service for any Data Source, with or without cause, effective sixty (60) days after written notice of termination is given to the other party. Customer accepts and agrees that, in the event (i) Customer terminates any order for convenience or (ii) Verizon terminates any order for Cause prior to the end of the order Term, then Customer will pay Verizon all unpaid fees payable under this Service Attachment and the applicable order for the remainder of such order Term. Customer will pay the invoice for such charges in accordance with the terms of the Agreement.

4.4 **Reinstatements**. If Customer elects to terminate an MSS - Analytics service for any Data Source or renew an MSS - Analytics service after it has ended, Verizon may require payment of the then-applicable service initiation fees to re-establish the MSS - Analytics service (e.g., set-up NRCs).

5. **Assumption of Risk.**

5.1 **Scanning Risks.** MSS - Analytics involves the use of network scanning technology that has inherent risks, including, but not limited to, the loss, disruption, or performance degradation of Customer's or a third party's business processes, telecommunications, computer products, utilities, or data (the "Scanning Risks"). When Customer requests network scanning, or any MSS - Analytics component utilizing network scanning, Customer authorizes Verizon to perform the network scanning and assumes all risk for adverse consequences resulting from or associated with such component of MSS - Analytics. Verizon will take reasonable steps to mitigate these Scanning Risks; however, Customer understands that these Scanning Risks are inherent in the provision of certain computer security services and the use of certain computer security products and cannot be eliminated. Customer will indemnify and defend Verizon for all costs and expenses related to a third party's claim of loss, damages and liabilities (including legal expenses and the expenses of other professionals) incurred by Verizon, resulting directly or indirectly from any claim attributable to or arising out of Verizon's use of network scanning technology (each, a "Scanning Claim"), including, without limitation, the use by Verizon of network scanning technology to analyze assets that are not controlled directly by Customer, including, without limitation, servers hosted by third parties. This obligation of Customer in connection with a Scanning Claim will not apply if Verizon's gross negligence or willful misconduct gave rise to such Scanning Claim.

5.2 **Change Requests.** Customer assumes all risks associated with Change Requests initiated by Customer. Verizon will deliver Change Requests strictly in accordance with the instructions provided by Customer. Verizon has no responsibility to provide technical advice to Customer in relation to the Change Requests, and the risks associated with such Change Requests.

6. **Third Party Products or Services.** The parties agree that Verizon will not be liable for any damages caused by hardware, software, or other products or services furnished by parties other than Verizon, its agents, subcontractors, or any damages caused by the products and/or services delivered by or on behalf of Verizon which have been modified, serviced, or otherwise attended to by parties other than Verizon or without Verizon's prior written and express consent. Customer acknowledges that Verizon will not be liable for any damages resulting, directly or indirectly, from any act or failure to act by Customer or any third party (including, without limitation, the non-performance, defaults, omissions or negligence of any third party that provides telecommunications services in the country or countries in which Customer's premises or systems are situated and other countries from, across, to or in respect which MSS - Analytics is provided by or on behalf of Verizon).
7. **Industry Alerts and Third Party Updates and Patches.** WITH REGARD TO SERVICES WHICH PROVIDE INFORMATION SHARING AND/OR INDUSTRY ALERTS, VERIZON DISCLAIMS ANY LIABILITY TO CUSTOMER, AND CUSTOMER ASSUMES THE ENTIRE RISK FOR (A) INFORMATION FROM THIRD PARTIES PROVIDED TO CUSTOMER WHICH TO THE BEST OF VERIZON'S INFORMATION, KNOWLEDGE AND BELIEF DID NOT CONTAIN FALSE, MISLEADING, INACCURATE OR INFRINGING INFORMATION, (B) CUSTOMER'S ACTIONS OR FAILURE TO ACT IN RELIANCE ON ANY INFORMATION FURNISHED AS PART OF MSS - ANALYTICS AND/OR (C) THE USE OF ANY THIRD PARTY LINKS, PATCHES, UPDATES, UPGRADES, ENHANCEMENTS, NEW RELEASES, NEW VERSIONS OR ANY OTHER REMEDY SUGGESTED BY ANY THIRD PARTY AS PART OF MSS - ANALYTICS.
8. **Verizon Materials.** If in connection with the provision of MSS - Analytics Verizon installs or provides any hardware or software ("Verizon Materials"), then Customer will use the Verizon Materials for internal purposes only as further defined in this Service Attachment. Customer will not distribute, reproduce, or sublicense the Verizon Materials. Customer will not reverse engineer, decompile, or disassemble or otherwise attempt to discover source code of the Verizon Materials. Verizon has the right to revoke the use of the Verizon Materials at any time. In such event, Customer will, at its sole cost and expense, promptly return the Verizon Materials to Verizon. Customer's right to use the Verizon Materials automatically terminates upon termination of this Service Attachment or upon completion of the portion of MSS - Analytics for which the Verizon Materials are provided.
9. **Confidential Information.** Customer acknowledges that the following information constitutes "Confidential Information" hereunder: (a) the methods, systems, data and materials used or provided by Verizon in connection with the provision of MSS - Analytics and (b) the results of Verizon's assessment of Customer and all reports issued by Verizon in connection with such results including, without limitation, security analyses and insight ("Net Intel Information"). Customer will disclose Net Intel Information only to Customer employees with a "need to know" for the purposes set forth in this Service Attachment and who are bound to confidentiality obligations at least as restrictive as those set forth in the Agreement and this Service Attachment. In no event may Customer use lesser efforts to protect Net Intel Information from use or disclosure not permitted under the Agreement than it uses to protect its own highly-sensitive confidential information, or less than reasonable efforts. The term "Confidential Information" will not include information that is comprised of statistical information, or other aggregated information regarding security vulnerabilities, security configurations and the like insofar as such information does not identify Customer or Customer's computer network or computer systems.
10. **Encryption Approvals in India.** Encryption functionalities associated with the management service of MSS - Analytics may only be provided to customers that have obtained permission from the Indian Department of Telecommunications or other Indian governmental authority or officer specially designated for the purpose. Customer is solely responsible for obtaining such approvals. Customer hereby indemnifies and hold harmless Verizon, from and against any claims, suits, judgments, settlements, losses, damages, expenses (including reasonable attorneys' fees and expenses), and costs (including allocable costs of in-house counsel) asserted against or incurred by Verizon arising out of a failure by Customer to comply with the restrictions described in this clause or as otherwise imposed by applicable laws and regulations of India pertaining to the use of encryption in India.

Part V: Service Level Agreement

1. **Key Performance Indicators.** This SLA defines the service metrics for which Customer has the right to receive credits ("Service Credits") in case Verizon fails to meet such metrics. In relation to a particular Data Source, the SLA will become effective when Verizon has issued the Ready for Operations notice.
   1.1 **Security Incident Escalation**

	Communication	**Communication**	**Reporting**
Channel	Email	Phone Email	Security Dashboard
Information Type	Incident Report - Insufficient Info	Incident Report - Harmful Attack	Security Dashboard
Reference Time	SMC Time Stamp	SMC Time Stamp	SMC Time Stamp

Response Time	≤ 30 minutes	≤ 15 minutes	Refreshed every 15 minutes
Contact Person	Authorized Users	Authorized Users	Authorized Users

1.1.1 **Security Incident Escalation Service Credits**

Response Time	Target Level ≤ X/Y	Service Credit
Incident Report - Insufficient Info > 30 minutes, ≤ 120 minutes	≤ 5 / 100	1
Incident Report - Insufficient Info > 120 minutes	0/month	2
Incident Report - Harmful Attack > 15 minutes, ≤ 60 minutes	≤ 1/100	1
Incident Report - Harmful Attack > 60 minutes	0/month	2

1.2 **Regular Change Request**

Regular Change Request	Timeframe
Accepted	≤ 24 hours after request
Implementation	During Maintenance Window

1.1.2 **Regular Change Request Service Credits**

Response Time	Target Level ≤ X/Y	Service Credit
Acceptance > 24 hours	≤ 1/10	1

2. **Service Credits Amount.**
   2.1 Subject to the conditions and exclusions set forth herein, Verizon will pay the applicable Service Credits as provided above. Service Credits will be calculated monthly. Service Credits are only available one month after RFS.
   2.2 One Service Credit equals the pro-rated charges for one day of the applicable MRC payable for the affected Serviced Device.
   2.3 The Target Level ≤ X/Y means that if Verizon exceeds the target response time X time(s) out of Y instances per month then the Customer may be eligible for a Service Credit.

3. **Service Credit Claims.**
   3.1 Customer must notify Verizon within 30 Business Days following a month where an SLA metric has not been met. No Service Credits will be issued if Verizon is not notified.
   3.2 Verizon will verify any requested Service Credit, and will confirm the amount of the credit, if applicable. Verizon's Service Credit calculation is the final and definitive assessment of any credit payable.
   3.3 Service Credits will be offset against future charges.

4. **Service Credit Conditions**
   4.1 If a number of unmet service metrics arise out of the same event, Customer will be entitled to the highest value Service Credit for one unmet metric.
   4.2 The total number of Service Credits for an affected Serviced Device may not exceed 50% of the MRC.
   4.3 Verizon will not pay Service Credits if the failure to meet service metrics is, directly or indirectly, due to:
   - A failure by Customer (or an entity under Customer's control) to comply with Customer's obligations as described herein.
   - The non-performance, default, error, omission, or negligence of any entity not under Verizon's reasonable control (such as, but not limited to, failure of any of Customer's third party providers of telecommunications services or problems with equipment Customer has provided).
   - The performance of routine maintenance work on a Serviced Device, service equipment at Customer's location, or on any of the equipment used to provision MSS - Analytics service during the applicable Maintenance Window or emergency maintenance.
   - Tests performed or commissioned by or on behalf of Customer (e.g. Urgent Change Requests); and/or
   - Any Force Majeure event.

Part VI: Definitions

24x7	Nonstop service, 24 hours a day, 7 days a week, 365 (366) days a year, independent of time zones and local or international public holidays.
Applicable Rates	The rates that apply for professional services work not covered under this Service Attachment. All such work is subject to the execution of a separate written agreement that describes the activities and the Applicable Rates for performing such work.
Authorized Contacts	Customer personnel authorized by Customer to access the Security Dashboard and to interact with Verizon.
Business Days	Monday through Friday, from 00:00 UTC to 24:00 UTC (Universal Time Code).
Business Hour	One hour during a Business Day. For example, a request coming in at 6:30pm London time and handled "within 4 Business Hours" is handled before 10:30pm London time. The phrase "within 24 Business Hours" means "before the same time of the next Business Day."
Change Request	A request from Customer or Verizon for a change to the SEAM policy, security analytics policy, Rule Set, configuration, Service Context or for a Security Upgrade.
Connection Kit	Equipment installed on the Customer's premises used to set up secured monitoring and/or management connections between the Data Sources and one or more Security Management Centers.
COTS/GOTS	Common or Commercial Off-the-Shelf/Government Off-the-Shelf product. A product, typically hardware or software, developed, marketed, sold and maintained by a specialist business, e.g., Microsoft Windows OS is a COTS product. GOTS products are often developed by government agencies (either in-house or via a specialist contractor paid by that agency) and are preferred by the government for use as all elements of the product can be controlled and built for government purposes.
Customer Environment	The network and/or information technology infrastructure in which Customer Data Sources reside.
Data	Machine-generated information that can be digitally transmitted and processed.
Data Source	Any Customer-designated source, including devices or services that generate Data. Data Sources include both traditional and non-traditional security devices, e.g., firewalls, intrusion detection and prevention devices, proxies, Unified Threat Management (UTM) devices, SIEMs, management stations, application logs, Security as a Service-based services, Active Directory, DHCP logs, etc. Data Sources can be configured on Customer's premises, with a third-party service provider or in the cloud.
Exploit	A method to use a Vulnerability to gain unauthorized access to functions, data, or privileges with malicious intent. An exploit can include a script, virus, Trojan, or a worm. The exploit is mainly defined by the way it replicates and spreads. An attack is the use of an Exploit. • A script refers to a document with steps to manually find and exploit vulnerabilities. A script is replicated by publishing it. • A virus refers to malicious software attached to a medium (e.g., files, removable media, documents). A virus replicates using this medium. • A Trojan refers to malicious software embedded in applications. The Trojan will not replicate itself; it spreads with the application. A worm refers to a self-contained program (or set of programs) that spreads copies to other computers. A worm can spread through network connections and emails in a matter of hours.
High Availability with Active/Active mode:	A configuration of two or more devices in a load balancing setup with all the devices passing network traffic. In case of failure of one device, the other device(s) either manually or automatically takes over the device functions of the failed device. This configuration is supported on a limited basis based on specific network architectures and Serviced Devices. Verizon will review and approve, if applicable, during the pre-sales design phase.
High Availability with Active/Passive mode:	A redundant configuration of two devices with duplicate software and data not necessarily co-located where the 'passive' device is activated manually or automatically when the 'active' device fails.
Incident Record Communication	A record in the system that tracks and drives the workflow of Incidents during their lifecycle to closure.
Login	IDs, account numbers, personal identification numbers or codes, passwords, digital certificates or other means of authentication.
Logs	A collection of various IT, compliance, network, application, and security related information created by Subordinate Devices.

Maintenance Window	A time window agreed between the Customer and Verizon for Verizon's performance of maintenance or management services on the Serviced Devices. During a Maintenance Window, the Serviced Devices and/or MSS - Analytics services may be temporarily disrupted or unavailable. Maintenance windows are limited to a maximum of 6 hours per maintenance window.
Major Change Request	A Change Request that involves any of the following: • Changes to the IP addresses of a Data Source. • Changes estimated to require more time than available in a Maintenance Window.
Monthly Data Volume Report	A report that summarizes the amount of data Customer is sending to Verizon for analysis. The report includes both daily and monthly data volume totals and is provided to Customer via the Security Dashboard.
Order Confirmation Date	Verizon will confirm Customer's order via email and the date of this email is the "Order Confirmation Date". The Order Confirmation will confirm the MSS service(s) requested.
Other Incident Ticket	A ticket for service related incidents logged with Verizon and created by the Customer or Verizon.
Project Manager	A Verizon-designated person who will act as the central point of contact throughout the MSS - Analytics implementation process and MSS - Analytics staging services, if applicable. The Project Manager will be responsible for managing the schedule and will also collaborate with the Customer to develop a project plan that will specify resources, dates, times, and locations for the tasks described in the project plan. The Project Manager also is responsible for managing the change control process.
Refresh Rate	The rate at which information on the Security Dashboard is refreshed. The Refresh Rate varies dependent on the type of information and the Serviced Device to which the information relates. • In general, Security and Health Incidents are updated on the Security Dashboard at a Refresh Rate of 15 minutes. • Statistics of Serviced Devices are refreshed on a daily basis. • Updates to Service Requests are reflected on the Security Dashboard as soon as changes are made to the status or comments are added, as per change management process.
Regular Change Request	A Change Request that Verizon will review and accept within 24 hours of submission and implement in the next Maintenance Window, provided that the minimum time between Customer's submission of a Regular Change Request and Verizon's implementation of such request will be 48 hours.
RFI	Request for Information – A customer inquiry regarding a Serviced Device or Data Source. Customers are charged one Service Ticket per RFI, unless the inquiry is related to an existing escalated incident, in which case no Service Tickets are charged.
RFO	Ready For Operations - The date (following RFS) that Verizon sends RFO notice to Customer and informs Customer that the Serviced Device security analytics policy have been fine-tuned and the escalation parameters, Service Context, and procedures have been set as mutually agreed. The SLA is effective as of this date. RFO is given per Serviced Device.
RFS	Ready For Service - The date on which Verizon starts providing the MSS – Analytics service on a Serviced Device. The RFS may vary for each MSS – Analytics service
Risk Correlation	Comparing data from multiple sources to find patterns and relationships that may point to attacks and abuse. Risk Correlation of Threats, Vulnerabilities and Assets.
Security Analytics Platform	Verizon's security analytics platform that uses COTS/GOTS hardware/software to process data and events from Customer Data Sources. Platform functions include: • Data and Log Processing, • Event Processing • Incident Handling • Vulnerability and Asset Processing • Health Monitoring.

SEAM	State and Event Analysis Machine – Proprietary Software used by Verizon. Its functions include: • Classification – giving Events a first classification, using Verizon proprietary Event Classification Policy Language, filtering out false positives or Events related to vulnerabilities absent in the targeted environment. • Workflow management – recording the activities for an Incident. • Information management – managing the information needed to examine, evaluate, and classify Incidents. • User management – defining the views and authorization levels of users.
Security Content	The rules, use cases, policies, threat identification capabilities, queries, and Threat Intelligence used within MSS - Analytics to identify potential Security Incidents.
Security Dashboard	Customer portal where customers can have a near-real-time view on the Events/Incidents being processed, and where they can view the company's security posture and effectiveness of the Security Devices and services at various levels.
Security Event ("Event")	A data record produced by Verizon's security analytics platform based on Verizon's proprietary threat detection policies.
Security Incident ("Incident")	A single Event or a series of Events that have been aggregated and correlated based on Verizon's proprietary threat detection policies. A Security Incident may represent an attack.
Security Upgrade	Changes to application software program to fix a security weakness or defect and which is generally released by the Serviced Device manufacturer as a Security Patch. A Security Upgrade includes signature or threat content updates.
Service Context	A set of documents with version control, posted on the Security Dashboard, containing information about the Customer that Verizon uses for the provisioning of MSS - Analytics to the Customer. The Service Context is setup during the service initiation phase and is maintained via the change management process. Customer can also add or update host information in the Service Context. The Service Context may include one or more of the following: • Authorized User details and authorization procedure for escalation, notification, and reporting • Service Description • Escalation, notification, reporting, and change control processes • Authorized Users • Information on maintenance and support contracts • Timeframe of Maintenance Windows • Roles and Responsibilities in the form of a RACI Matrix for complex and/or custom solutions • Network topologies and asset inventories of systems
Service Ticket	A unit for charging certain usage-based services under MSS - Analytics. A number of Service Tickets are included in each MSS - Analytics service by default.
SLA (Service Level Agreement)	The agreement setting forth the specific service levels and the terms and conditions for receiving Service Credits if Verizon were to fail to meet these service levels.
SMC (Security Management Center)	A data center that hosts the Managed Security Services platform and the systems for monitoring, managing, or supporting the Serviced Devices. The SMC includes: equipment to connect to the Connection Kit, management stations, hosts the virtual Local Event Collector, SEAM engines, Verizon's security analytics platform, and Security Dashboard., and back-end systems such as back-up devices, file servers, and terminal servers.
SMC Time Stamp	A time stamp recorded by Verizon at the SMC and reported on the Security Dashboard. The time stamps are used as the reference for measuring the Service Level Agreement. The SMC Time Stamp is recorded in UTC and synchronized worldwide using the Network Time Protocol ("NTP").
SOC (Security Operations Center)	A data center where the Verizon security analysts work.
SSL Certificate	A digital certificate is compliant with x.509v3, RFC 2459, RFC 3280, and RFC 3039 and includes at a minimum: • A public key • The identity or unique pseudonym of the certificate subscriber who owns and holds the private key matching the listed public key • The Issuer's identity • A start date and expiration date • A reference to the governing policy of the Issuer

Threat	A (suspected) use of an Exploit, or the (suspected) presence of a Vulnerability in the configuration, platform, or application code. A Threat can be an infection by a worm or virus, or it can be a targeted attack. Exploits can also be combined into Blended Threats, exploiting multiple security weaknesses or defects.
Threat Intelligence	Strategic, tactical, and operational intelligence used to develop applied detection policies and perform multi-factor incident correlation, so that only those threats that pose a significant risk are identified.
Threat Signature	Code used to recognize a Threat by its pattern. A Threat Signature may contain algorithms to detect dynamically changed malicious behavior, combat obfuscation, or impersonation.
User Interface	A web-based portal, dashboard, or other electronic means to share information and reports with customers that pertains to Security Incidents that are identified and escalated to the customer.
UTC (Coordinated Universal Time)	Universal Time indication standardized by the Bureau International des Poids et Measures (BIPM) and defined in CCIR Recommendation 460-4. The UTC is the time indicated on atomic clocks. Verizon consults and uses it for its Sacs via the Internet protocol NTP. The UTC code uses the 24-hour clock. 4 pm (afternoon) is equal to 16:00 UTC. Depending on the daylight savings period, the UTC is 4 or 5 hours ahead of Eastern Standard Time (EST), and 1 or 2 hours behind Central European Time (CET).
Vulnerability	A weakness or defect that can be exploited to gain access to data, functions, or privileges violating the intended authorization. Vulnerabilities can range from defects in application or system software (e.g., bugs), in the user administration (e.g., non-protected user accounts), in the configuration (e.g., unintended network or file access), in the policy and rule set definition (e.g., unrestricted open ports or exposed IP addresses), etc. The combination of all vulnerabilities of a given system or infrastructure is the exposure.
Workaround	An alternative function or method, often using a temporary patch or reconfiguration, to achieve a result equivalent to the original function or method.

EXHIBIT 2
TO ATTACHMENT A OF
MEMBER PARTICPATION AGREEMENT

STATEMENT OF WORK

Client Security Engineering Analyst

The primary responsibility of the Client Security Engineer (CSE) is to aggregate data, identify and analyse unusual and interesting patterns, and provide decision analysis back to the client, what can result in changes to the client correlation policy. Secondary responsibilities would include, but would not be limited to, incident response support, custom reporting, filtering of risk intelligence specific for the client environment, uploading vulnerability details into Verizon MSS SEM (if available), risk/compliance scoring.

The CSE is tasked with lifecycle ownership of the environment and works closely with Security Operations Center and back office MSS teams to provide 3rd and/or 4th level operational support, problem resolution, and identify production pain points.

- The team understands how to quantify risk using threat likelihood, implementation state, and business impact variables. The team also understands that compliance and risk scoring are not the same. Even though they complement each other, they have to be illustrated separately.
- The team understands how to prioritize remediation efforts based on business need, compliance need, and/or risk reduction need.
- The team understands how to analyse discovery scan data and vulnerability data to determine unusual use configurations, discovery of aged software, and proper identification of high-severity vulnerabilities. In most cases, the team will identify and remove false positive findings and/or downgrade certain vulnerabilities based on Verizon Risk Intelligence.
- The team understands how to upload vulnerability details into the MSS SEM engine, analyse Level 0 through Level 4 incidents, and tune the MSS correlation engine.
- The team understands how to define action plans that are easy to implement, effective at reducing risk, and as much as possible will take advantage of existing people, processes, and technologies.

In concert, the Verizon CSE role will complement the MSS Security Monitoring service, and provide customer with a personal security analyst contact, that will deliver:

- Weekly status calls with the Client CSIRT team and/or security officers to discuss risk intelligence, incidents, vulnerability details, correlation change request, implementation state, compliance state, and/or risk state.
- Detailed monthly Incident Reports. The analytical outcome of these reports will be used for a further discussion with client on the customization of the security monitoring policy.
- Customization of the security monitoring policy to align to customer monitoring strategies
- Recurring and adhoc Risk Intelligence information advice :
    - Customer will – as any other Verizon MSS customer – receive from Verizon a weekly Intelligence Summary (INTSUM), monthly invites to Verizon Risk Briefings, adhoc publication of hype or hot analysis for emerging vulnerabilities or exposures.
    - The CSE will further filter these alerts and customise based on the client's environment:
        - Ad-hoc Emergency global threat information tuned for the customer environment. (e.g., Heartbleed how-to focus for client)
        - Append the weekly INTSUM report with Retail sector specific or client specific focus/prioritisation advice, to discuss during weekly status calls.
        - Forwarding of vulnerability alerts for the MSS supported portfolio, specifically filtered for the Client environment (e.g., An urgent recommended patch for a Palo Alto Networks firewall)

- The CSE will also be available (US business hours) to discuss the details and relevance of all risk intelligence publications.
- The CSE acts as a trusted technical advisor role, and is available to discuss all technical service aspects, with the Verizon SSA and customer.
- The CSE will also assist and support in the setup and transition of service devices including:
  - Review and strategy of integrating logging recommendations that the customer was given for audit compliance.
  - Helping ready customer environment for the ingestion of log data into the Verizon MSS service.
  - Logging volume and evaluating the need for compression to keep throughput to reasonable for data sent to VZ in transit across IPSec.
  - Evaluate and assist with setup of a VZ Collector if needed.
  - Evaluate and assist with setup WEC for Windows Systems ingestion with Snare as necessary.
  - Evaluate and assist with setup/config to facilitate syslog for Linux and other system log consolidation as necessary.
  - Create and implement strategy for phases of the project up to and beyond the RFO of the devices while working with Verizon MSS PM.
    - Work with the GARM SOC and PLCE to tune to maximize the value of the source logs after RFO for customer satisfaction.

During the service setup phase:

- the CSE will assist the Verizon project team, with the technical coordination and documentation aspects of the log onboarding phase, including the provisioning of log forward instructions towards the client.
- CSE will also participate in the training on the Security Monitoring service which the Verizon SSA will setup for the customer team that will access the Verizon Security Dashboard, and specifically for the client CSIRT on interaction procedures with SOC and CSE.

There are four levels available: 0.25 FTE, 0.5 FTE, 0.75 FTE and 1.0 FTE, depending on the customer environment and requirements.

END OF EXHIBIT