MEMORANDUM OF AGREEMENT
BETWEEN THE CENTER FOR INTERNET SECURITY/MULTI-STATE INFORMATION SHARING AND ANALYSIS CENTER
AND
COMMONWEALTH OF VIRGINIA
VIRGINIA INFORMATION TECHNOLOGIES AGENCY
FOR
CYBER SECURITY SERVICES
(Federally Funded Services)

This MEMORANDUM OF AGREEMENT (Agreement) by and between the Center for Internet Security, Inc. ("CIS"), operating in its capacity as the Multi-State Information Sharing and Analysis Center (MS-ISAC), located at 31 Tech Valley Drive, East Greenbush, NY 12061-4134, and Commonwealth of Virginia, Virginia Information Technologies Agency (Entity) with its principal place of business at: 11751 Meadowville Lane, Chester, VA 23836 for Cyber Security Services, as defined herein below (CIS and Entity collectively referred to as the "Parties").

WITNESSETH:

WHEREAS, In its role as the MS-ISAC, CIS has been recognized by the United States Department of Homeland Security (DHS) as a key Cyber Security resource for all fifty states, local governments, United States territories, and tribal nations (SLTT); and

WHEREAS, CIS operates a twenty-four hours a day, seven days per week (24/7) Security Operations Center (SOC); and

WHEREAS, CIS has entered into an agreement with the federal government to provide base level Cyber Security Services to SLTT; and

WHEREAS, the Entity is one of the recipients of the Cyber Security Services.

NOW, THEREFORE, in consideration of the mutual covenants contained herein, the Parties do hereby agree as follows:

I. Purpose

The purpose of this agreement is to set forth the mutual understanding between Entity and CIS with respect to the provision of Cyber Security Services to Entity.

II. Definitions

A. Security Operation Center (SOC) – 24 X 7 X 365 watch and warning center that provides network monitoring, dissemination of cyber threat warnings and vulnerability identification and mitigation recommendations.

B. Cyber Security Services (CSS) – Combined Netflow and intrusion detection system monitoring and analysis of related data, and delivery and management of associated devices, hardware and software necessary for delivery of CSS. Also referred to as Albert monitoring services. For purposes of clarification, the performance of the Cyber Security Services does not require or involve the decryption of any encrypted traffic.

III. Consideration

Federally Funded Cyber Security Services - Pursuant to the agreement with the federal government, CIS is providing Cyber Security Services and associated security devices at no charge to Entity.

IV. Responsibilities

Appendix A, which is attached hereto and incorporated herein, contains the specific responsibilities for Entity and CIS regarding the CSS. Entity understands and agrees that, as a condition to commencement of CSS under the terms of this Agreement, it must:

A. agree to comply with the terms and conditions applicable to Entity as set forth in Appendix A; and

B. execute the Entity Certification form attached as part of Appendix A.

V. Title

CIS will at all times retain title to hardware and/or software provided to Entity during the Term of this Agreement. Upon termination or expiration of this Agreement, Entity will return all hardware and/or software provided under this Agreement within thirty (30) days of such expiration or termination.

VI. Term of this Agreement

This Agreement will commence on the date it is signed by both Parties, and shall continue in full force and effect until terminated (the "Term"). Either party may terminate this Agreement by providing written notice to the other party ninety (90) days prior to termination.

Additionally, if during the Term of this Agreement, Entity makes changes to its hardware or network configuration in such a manner that CIS is no longer able to provide the CSS to Entity, CIS shall have the ability to terminate this Agreement upon written notice to Entity.

The ability and obligation of CIS to provide these Cyber Security Services and devices to the Entity is, at all times, contingent on the availability and allocation of federal funds for this purpose.

VII. Amendments to this Agreement

This Agreement may only be amended as agreed to in writing by both Parties.

VIII. No Third Party Rights

Nothing in this Agreement shall create or give to third parties any claim or right of action of any nature against Entity or CIS.

IX. Disclaimer

Both Parties disclaim all express and implied warranties with regard to the CSS provided for herein, and neither party to this Agreement assumes any responsibility or liability for the accuracy of the information which is the subject of this Agreement, or for any act or omission or other performance related to the CSS provided under this Agreement, including any act or omission by contractors or subcontractors of CIS.

X. Confidentiality Obligation

CIS acknowledges that information regarding the infrastructure and security of Entity information systems, assessments and plans that relate specifically and uniquely to the vulnerability of Entity information systems, the results of tests of the security of Entity information systems insofar as those results may reveal specific vulnerabilities or otherwise marked as confidential by Entity ("Confidential Information") may be provided by Entity to CIS in connection with the services provided under this Agreement. The Entity acknowledges that it may receive from CIS trade secrets and confidential and proprietary information ("Confidential Information"). Both Parties agree to hold each other's Confidential Information in confidence to the same extent and the same manner as each party protects its own confidential information, but in no event will less than reasonable care be provided and a party's information will not be released in any identifiable form without the express written permission of such party or as required pursuant to lawfully authorized subpoena or similar compulsive directive or is required to be disclosed by law, provided that the Entity shall be required to make reasonable efforts, consistent with applicable

law, to limit the scope and nature of such required disclosure. CIS shall, however, be permitted to disclose relevant aspects of such Confidential Information to its officers, employees, agents and CIS's cyber security partners, including federal partners, provided that such partners have agreed to protect the Confidential Information to the same extent as required under this Agreement. The Parties agree to use all reasonable steps to ensure that Confidential Information received under this Agreement is not disclosed in violation of this Section. These confidentiality obligations shall survive any future non-availability of federal funds to continue the program that supports this Agreement or the termination of this Agreement.

XI. Notices

A. All notices permitted or required hereunder shall be in writing and shall be transmitted either:

1. via certified or registered United States mail, return receipt requested;
2. by facsimile transmission;
3. by personal delivery;
4. by expedited delivery service; or
5. by e-mail with acknowledgement of receipt of the notice.

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

CIS
Name: Mark Perry
Title: Program Executive, Partner Engagement
Address: Center for Internet Security, Inc.
The Multi-State Information Sharing and Analysis Center
31 Tech Valley Drive
East Greenbush, NY 12061-4134

Telephone Number: (518) 880-0699
Facsimile Number: (518) 283-3216
E-Mail Address: mark.perry@cisecurity.org

Entity
Name: Michael Watson
Title: Chief Information Security Officer
Address: 11751 Meadowville Lane
Telephone Number: (804) 416-6030
Facsimile Number:
E-Mail Address: michael.watson@vita.virginia.gov

service or certified or registered United States mail, as of the date of first attempted delivery at the address and in the manner provided herein, or in the case of facsimile transmission or email, upon receipt.

C. The Parties may, from time to time, specify any new or different contact information as their address for purpose of receiving notice under this Agreement by giving fifteen (15) days written notice to the other Party sent in accordance herewith. The Parties agree to mutually designate individuals as their respective representatives for the purposes of receiving notices under this Agreement. Additional individuals may be designated in writing by the Parties for purposes of implementation and administration, resolving issues and problems and/or for dispute resolution.

The foregoing has been agreed to and accepted by the authorized representatives of each party whose signatures appear below:

CENTER FOR INTERNET SECURITY, INC.	**COMMONWEALTH OF VIRGINIA VIRGINIA INFORMATION TECHNOLOGIES AGENCY**
Federal Identification No.	Federal Identification No.
52-2278213	54-1074144
By: Thomas Duffy	By: Doug Crenshaw
Name: Thomas Duffy	Name: Doug Crenshaw
Title: Sr. VP of Operations & Services	Title: Info-Security Mgr
Date: 1/20/16	Date: 1/5/16

Appendix A

CSS Responsibilities

I. **Entity Responsibilities** - Entity acknowledges and agrees that CIS's ability to perform the Cyber Security Services provided by CIS for the benefit of Entity is subject to Entity fulfilling certain responsibilities listed below. Entity acknowledges and agrees that neither CIS nor any third party provider shall have any responsibility whatsoever to perform the Cyber Security Services in the event Entity fails to meet its responsibilities described below.

A. For purposes of this Agreement, Entity acknowledges and agrees that only those security devices supported by CIS fall within the scope of this Agreement.

B. Entity shall provide logistic support in the form of rack space, electricity, Internet connectivity, and any other infrastructure necessary to support communications at Entity's expense.

C. Entity shall provide the following to CIS prior to the commencement of service and at any time during the term of the Agreement if the information changes:

1. Current network diagrams to facilitate analysis of security events on the portion(s) of Entity's network being monitored. Network diagrams will need to be revised whenever there is a substantial network change;
2. In-band access via a secure Internet channel to manage the device(s).
3. Outbound access via a secure Internet channel for log transmission.
4. Reasonable assistance to CIS as necessary, to enable CIS to deliver and perform the CSS for the benefit of Entity;
5. Maintenance of all required hardware, virtual machines, or software necessary for the sensor located at Entity's site, and enabling access to such hardware, virtual machines, or software as necessary for CIS to provide the CSS;
6. Public and Private IP address ranges including a list of servers being monitored including the type, operating system and configuration information; and list of IP ranges and addresses that are not in use by the Entity (DarkNet space);
7. Completed Pre-Installation Questionnaires (PIQ). The PIQ

will need to be revised whenever there is a change that would affect CIS's ability to provide the Cyber Security Services;

8. Accurate and up-to-date information, including the name, email, landline, mobile, and pager numbers for all designated, authorized Point of Contact(s) who will be provided access to the portals, and;
9. The name, email address, and landline, mobile, and pager numbers for all shipping, installation and security points of contact.

D. With respect to the shipping and delivery of any required hardware, Entity agrees to the following:

1. For any hardware shipped directly to Entity, upon receipt of the hardware, Entity shall contact CIS to confirm the serial number of the hardware. Upon confirmation of the serial number, CIS will ship an identification tag to Entity. Entity agrees to place the identification tag on the hardware as per the accompanying instructions, and upon placement of the identification tag, to confirm in writing to CIS that the tag has been placed on the hardware.
2. In certain instances, CIS may ship hardware and software to Entity prior to the final execution of this Agreement. Notwithstanding the foregoing, Entity acknowledges that commencement of CSS is contingent on the execution of this Agreement by the parties.

E. During the term of this Agreement Entity shall provide the following:

1. Written notification to CIS SOC (SOC@MSISAC.ORG) at least thirty (30) days in advance of changes in hardware or network configuration affecting CIS's ability to provide Cyber Security Services, or a change to the physical location of the hardware; any notice relating to change in physical location shall include the new physical address of the hardware;
2. Written notification to CIS SOC (SOC@MSISAC.ORG) at least twelve (12) hours in advance of any scheduled downtime or other network and system administration scheduled tasks that would affect CIS's ability to provide the service;
3. A completed Escalation Procedure Form including the name, e-mail address and 24/7 contact information for all designated Points of Contact (POC). A revised Form must be submitted when there is a change in status for any POC;
4. Sole responsibility for maintaining current maintenance and technical support contracts with Entity's software and

hardware vendors for any device affected by CSS that has not been supplied by CIS;

5. Active involvement with CIS SOC to resolve any tickets requiring Entity input or action;
6. Reasonable assistance in remotely installing and troubleshooting devices including hardware and communications,
7. Upon reasonable notice from CIS and during normal business hours, access for CIS to inspect the hardware.

8. Response to biennial written confirmation notice from MS-ISAC as to the physical location of all hardware provided by CIS.

F. Certification. Entity shall complete the attached Entity Certification documenting compliance with the following:

1. That the Entity provides notice to its employees, contractors and other authorized internal network users (collectively, "Computer Users") that contain in sum and substance the following provisions:

   (a) Computer Users have no reasonable expectation of privacy regarding communications or data transiting, stored on or traveling to or from Entity's information system; and
   (b) Any communications or data transiting, stored on or traveling to or from the Entity's information system may be monitored, disclosed or used for any lawful government purpose; and

2. That all Entity Computer Users execute some form of documentation or electronic acceptance acknowledging his/her understanding and consent to the above notice. Examples of notice documentation include, but are not limited to:

   a) log-on banners for computer access with an "I Agree" click through;
   b) consent form signed by the Computer User acknowledging Entity's computer use policy; or
   c) computer use agreement executed by the Computer User.

II. CIS Responsibilities

A. CIS will be responsible for the correct functioning of managed devices.

B. CIS shall be responsible for the purchase of certain hardware, and shall arrange for the shipping of such hardware to a location designated by Entity. Upon notice from Entity that the hardware has been delivered and upon confirmation of the serial number of the hardware, CIS shall be responsible for providing Entity with an identification tag to be placed on the hardware.

C. CIS will provide the following as part of the service:

1. Analysis of logs from monitored security devices for attacks and malicious traffic;
2. Analysis of security events;
3. Correlation of security data/logs/events with information from other sources;
4. Notification of security events per the Escalation Procedures provided by Entity.
5. Ensuring that all upgrades, patches, configuration changes and signature upgrades are applied to managed devices. CIS will provide the appropriate license and support agreements for the upgrade for devices provided by CIS. The Entity is responsible for maintaining the appropriate license and support agreements for devices own by the Entity.

D. Access to Stored Flow Data. CIS shall provide access to normalized logs, security events and netflow data through batch queries.

E. CIS Security Operation Center. CIS will provide 24/7 telephone (1-866-787-4722) availability for assistance with events detected by the CSS.

F. Biennial Confirmation for Hardware Location. Every two years, CIS will send Entity a request for confirmation of the physical location of the hardware provided as part of the CSS, including description, serial number and address of physical location of hardware.

ENTITY CERTIFICATION

On behalf of Virginia Information Technologies Agency ("Entity"), I hereby certify the following:

1. Entity provides notice to its employees, contractors and other authorized internal network users ("collectively "Computer Users") that contain in sum and substance the following provisions:

   -Computer Users have no reasonable expectation of privacy regarding communications or data transiting, stored on or traveling to or from Entity's information system; and

   -Any communications or data transiting, stored on or traveling to or from the Entity's information system may be monitored, disclosed or used for any lawful government purpose.

2. All Entity Computer Users execute a form of documentation or electronic acceptance acknowledging his/her understanding and consent to the above notice.

3. I am authorized to execute this Certification on behalf of Entity.

Dated this 11 day of January, 2016

Name: Michael Watson
Title: CISO