TOWN OF OCEAN VIEW

DELAWARE

October 4, 2023

TO: Mayor and Council

FROM: Carol S. Houck, Town Manager

SUBJECT: Support to Enter into a Memorandum of Agreement (MOA) for Services with The Delaware Department of Technology and Information (DTI)

BACKGROUND

The State of Delaware has procured the services of the Center for Internet Security (CIS) to be deployed among the local Towns and Cities across the state under a written agreement between the State of Delaware and in our case the Town of Ocean View.

In recent weeks, we have met with the Director of Risk Management and Governance Sandra Alexander to discuss this opportunity and decide whether it was in the Towns best interest to enter the MOA. If entered, certain cyber security monitoring services would be made available to the Town free of charge for one year as follows:

- Combined NetFlow and Intrusion detection system monitoring, with analysis of related data; event notification and delivery; and management of associated devises, including hardware and software necessary for service delivery.
- KnowB4 – Security Awareness Training deployment to Staff, Council and Committee members
- Delivered via the CIS Security Operating Center (24 x 7 x 365) and providing network monitoring, dissemination of cyber threat warnings, vulnerability identification and mitigation recommendations.

After the meeting our review team including me, Sergeant Carter (our in-house IT specialist) and Phil Malstrom, President of Diamond Computer Incorporated (our outsourced vendor for IT applications and backup operations) determined it was in the Towns best interest to take advantage of this year one savings and enhanced protection. Future years may also see a funding source available from the States Local Cyber Security Grants currently being developed. Further, Sergeant Carter has acknowledged he can provide the necessary information to facilitate the project and will serve as the Point of Contact for the project(s).

RECOMMENDATION

It is therefore recommended that Mayor and Council authorize the Town Manager to enter into a MOA (attached) with the State of Delaware Dept of Technology and Information (DTI) thereby enabling the Town of Ocean View to access year one deployment of cyber security monitoring services.

MEMORANDUM OF AGREEMENT FOR SERVICES

This MEMORANDUM OF AGREEMENT (MOA) by and between ______________________ with its principal place of business at: _____________________ ("State/Agency"), and ___________ , ("Local Entity") with its principal place of business at: ______________________________ is hereby entered into as defined herein below. (State/Agency and Local Entity each a "Party" and collectively referred to as the "Parties").

WITNESSETH:

WHEREAS, Center for Internet Security, Inc. ("CIS"), offers fee-based Services (as defined herein) to state and local government and elections entities and State/Agency has procured such Services to be deployed at Local Entity, subject to the terms and conditions set forth in a written agreement between State/Agency and CIS ("Agreement"), and

WHEREAS, section IV of said Agreement requires the execution of a MOA between State/Agency and Local Entity as a condition precedent to the delivery of such Services, and

WHEREAS, State/Agency and Local Entity wish to enter into this MOA to further set forth the duties and obligations of the Parties.

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

I. Definitions

A. Services. Combined Netflow and intrusion detection system monitoring, with analysis of related data; event notification and delivery; and management of associated devices, including hardware and software necessary for service delivery. Also referred to as **"Services".**

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

II. Local Entity Responsibilities

The Local Entity hereby agrees that it will undertake the following:

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

B. Local Entity shall provide the following to CIS prior to the commencement of

Services and at any time while receiving Services if the previously provided information changes:

1. Current network diagrams to facilitate analysis of security events on the portion(s) of Local Entity's network being monitored. Network diagrams will need to be revised whenever there is a substantial network change;

2. Other reasonable assistance to CIS, including, but not limited to, providing all technical information related to the Service reasonably requested by CIS, to enable CIS to perform the Albert Monitoring Service for the benefit of Local Entity;

3. Provide public and private IP address ranges including a list of servers being monitored including the type, operating system and configuration information, as well as a list of IP ranges and addresses that are not in use by Local Entity (DarkNet space);

4. Completed Pre-Installation Questionnaires (PIQ) in the form provided by CIS. The PIQ will need to be revised whenever there is a change that would affect CIS's ability to provide the Services;

5. Provide a completed Escalation Procedure Form including the name, e-mail address, and 24/7 contact information for all designated Points of Contact (POC).

6. The name, email address, and landline, mobile, and pager numbers for all shipping, installation and security points of contact.

C. During the period that Local Entity is receiving Services, Local Entity shall provide the following:

1. Written notification to CIS SOC (SOC@cisecurity.org) at least thirty (30) days in advance of changes in hardware or network configuration affecting CIS's ability to provide Services;

2. Written notification to CIS SOC (SOC@cisecurity.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 Albert Monitoring Service;

3. A revised Escalation Procedure Form when there is a change in status for any POC for the Local Entity.

4. Sole responsibility for maintaining current maintenance and technical support contracts with Local Entity's hardware vendors for any device affected by Services.

5. Local Entity shall provide active involvement with CIS SOC to resolve any tickets requiring Local Entity input or action; and

6. Reasonable assistance in remotely installing and troubleshooting devices including hardware and communications.

III. State/Agency Responsibilities

As consideration for the Services provided to Local Entity, State/Agency has agreed to pay to CIS the costs for such Services as set forth in the Agreement for the first year. The State does not have nor plan to have appropriations for year two and beyond ("succeeding years"). The Local Entity shall pay CIS the costs for such Services as set forth in the Agreement for the succeeding years. If the Local Entity does not obtain appropriation for the succeeding years, then the Agreement terminates for non-appropriation.

IV. Term of this MOA; Termination

A. Term. This MOA will commence on the date it is signed by the Parties (the "Effective Date"), and shall continue in full force and effect for as long as the Services are made available to Local Entity and appropriations are available under the Agreement (the "Term"), unless otherwise earlier terminated pursuant to the terms of this Section IV. If the Agreement between State/Agency and CIS is terminated by CIS for any reason, this MOA shall terminate as of the date of such termination of the Agreement. Unless this MOA is terminated early or extended in writing by the Parties, it shall terminate upon the expiration of the Term.

B. Termination. Either Party may terminate this MOA during the Term by providing written notice to the other Party at least ninety (90) days prior to termination. Either Party may terminate this MOA immediately for non-appropriations.

V. Force Majeure

No Party shall be liable for performance delays or for non-performance due to causes beyond its reasonable control.

VI. No Third-Party Rights

Except as otherwise expressly stated herein, nothing in this MOA shall create or give to third parties any claim or right of action of any nature against State/Agency or Local Entity.

VII. Assignment

No Party may assign their rights and obligations under this Agreement without the prior written approval of the other Party which approval shall not be unreasonably withheld, conditioned or delayed. This Agreement shall be binding upon and inure to the benefits of each Party and their respective successors and assigns.

VIII. Information Sharing

The Parties acknowledge that, as a condition precedent to the execution of this MOA, CIS shall share all incident notification reports involving Local Entity with State/Agency. This requirement shall remain in effect during the term of this MOA.

IX. Notices

A. All notices permitted or required hereunder shall be in writing and shall be transmitted either: via certified or registered United States mail, return receipt requested; by facsimile transmission; by personal delivery; by expedited delivery service; or 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:

<u>State/Agency</u>
Name:
Title:
Address:
Phone:
E-Mail:

<u>Local Entity</u>
Name:
Title:
Address:
Phone:
E-Mail:

B. Any such notice shall be deemed to have been given either at the time of personal delivery or, in the case of expedited delivery service or certified or 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 MOA by giving fifteen (15) days written notice to the other Parties sent in accordance herewith. The Parties agree to mutually designate individuals as their respective representatives for the purposes of receiving notices under this MOA. 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.

X. Non-Waiver

None of the provisions of this MOA shall be considered waived by any Party unless such waiver is given in writing by the other Parties. No such waiver shall be a waiver or any past or future default, breach or modification of any of the terms, provision, conditions or covenants of the MOA unless expressly set forth in such waiver.

XI. Disputes

Each party shall make a good faith effort to negotiate a resolution of any disputes between the parties related to this MOA.

XII. Governing Law

This MOA shall be construed and interpreted in accordance with the laws of the State of Delaware, and the venue of any action brought hereunder shall be in the Courts of Delaware.

XIII. Entire Agreement; Amendments

This MOA constitutes the entire understanding and agreement between the Parties with respect to the subject matter hereof and replace and supersede all prior understandings, communications, agreements or arrangements between the parties with respect to this subject matter, whether oral or written. This MOA may only be amended as agreed to in writing by all Parties.

XIV. Partial Invalidity

If any provision of this MOA be adjudged by a court of competent jurisdiction to be unenforceable or invalid, that provision shall be limited or eliminated to the minimum extent necessary so that this MOA shall otherwise remain in full force and effect and enforceable.

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

STATE/AGENCY	**LOCAL ENTITY**
By: ______________________	By: ______________________
Name: ______________________	Name: ______________________
Title: ______________________	Title: ______________________
Date: ______________________	Date: ______________________

Good Afternoon:

Please see below for an important message originating from The Cybersecurity and Infrastructure Security Agency (CISA).

Thanks

Sandra E. Ennis-Alexander, CISSP, MBCP
Director of Risk Management and Governance
Office of the Chief Security Officer
Department of Technology and Information
State of Delaware
302.739.9637 (phone)
302.677.7097

From: MS-ISAC Advisory <MS-ISAC.Advisory@msisac.org>
Sent: Monday, February 06, 2023 2:18 PM
To: MS-ISAC SOC <SOC@msisac.org>
Subject: Message from the MS-ISAC: Pending Royal Ransomware Campaign Targeting US Entities - TLP: AMBER

TLP:AMBER

TO: All MS-ISAC Members

DATE: February 6, 2023

The MS-ISAC is observing an uptick in SLTT targeting from the "Royal" ransomware variant, including recently reported incidents impacting K-12 school districts.

In an effort to inform membership about this ransomware, the MS-ISAC is sharing information from CISA regarding a pending Royal ransomware campaign.

Per CISA:

CISA has been made aware by multiple trusted industry partners of a pending Royal Ransomware campaign targeting a wide range of U.S. entities across multiple sectors, including SLTT entities. CISA has not independently verified this information but is confident in its reliability. We realize this message is light on specifics, but are sharing for early warning purposes. Please let us know if you have any questions!

What we know:

- Reports indicate the campaign started as soon as yesterday.
- We strongly suspect Royal used LinkedIn and other social media scraping to compile names from potential target organizations and then auto-generated or guessed the email addresses for compilation into target lists. **SLTT entities should be on the lookout for messages that go to non-existent addresses within their email domains.**
- It will begin with phishing emails aimed at deploying Cobalt Strike.
- Both BazarCall and a new version of Trickbot are expected to be used as initial infection vectors.
- Royal has used U.S. election related and partisan group (patriot group, for example) themes in past phishing campaigns. We expect similar phishing lures alongside new lures and subjects.
- Reports indicate Royal has procured an anti-virus related code-signing certificate that will give this campaign a marked advantage against most endpoint monitoring and security technology. CISA is working to identify the specific certificate.
- We expect the targeting of unmitigated/unpatched Microsoft Exchange and Log4J vulnerabilities.
- Expected TTPs for this campaign:
  - T1486 - Data Encrypted for Impact
  - T1106 - Native API
  - T1083 - File and Directory Discovery
  - T1140 - Deobfuscate/Decode Files or Information
  - T1489 - Service Stop
  - T1490 - Inhibit System Recovery

CISA recommends organizations reference the CISA/MS-ISAC Joint Ransomware Guide for defensive best practices and incident response guidance.

https://www.cisa.gov/stopransomware/ransomware-guide

Royal Ransomware Background Information

The Royal ransomware operation first emerged in September 2022 and is currently one of the most active variants across all sectors. According to open source reporting, this group started targeting organizations in January 2022 under the name “Zeon” before rebranding as Royal. As with many ransomware groups, Royal operates a data leak site where they list victims and threaten to leak stolen data if the ransom is not paid. Recent reporting indicates the group is encrypting Linux devices, specifically targeting VMware ESXi virtual machines, along with targeting Windows devices.

Royal uses a variety of initial access techniques ranging from malicious ads posing as legitimate software to callback phishing emails. Callback phishing emails involve social engineering to trick end users into calling a fake customer support phone number and then talking them through installing remote access software. In recent weeks, cybersecurity researchers at a cyber insurance provider reported that Royal is actively targeting a Citrix vulnerability, CVE-2022-27510.

The Royal ransomware operation reportedly leverages a variety of malware in its infection chains, most notably BATLOADER; however, IcedID, QakBot, Vidar Stealer, Ursnif, and

Bumblebee are also referenced in open source reporting related to Royal ransomware activity. Additionally, reporting indicates the group uses the Cobalt Strike post-exploitation tool.

The MS-ISAC will continue to monitor activity and reporting related to the Royal ransomware operation and update membership accordingly.

Sources:

- https://www.bleepingcomputer.com/news/security/new-royal-ransomware-emerges-in-multi-million-dollar-attacks/
- https://www.microsoft.com/en-us/security/blog/2022/11/17/dev-0569-finds-new-ways-to-deliver-royal-ransomware-various-payloads/
- https://www.at-bay.com/articles/likely-first-exploit-citrix-vulnerability/
- https://www.hhs.gov/sites/default/files/royal-ransomware-analyst-note.pdf
- https://www.bleepingcomputer.com/news/security/linux-version-of-royal-ransomware-targets-vmware-esxi-servers/

Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061

24x7 Security Operations Center
SOC@cisecurity.org - 1-866-787-4722

MS-ISAC® EI-ISAC®