MEMORANDUM OF AGREEMENT
BETWEEN THE CENTER FOR INTERNET SECURITY
AND
Hoke County Board of Elections
FOR
Endpoint Detection & Response (EDR) 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) and the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), located at 31 Tech Valley Drive, East Greenbush, NY 12061-4134, and Hoke County Board of Elections (Entity) with its principal place of business at: 423 E Central Ave, Raeford, North Carolina 28376 for EDR Services, as defined herein below (CIS and Entity collectively referred to as the "Parties").

- In its role as the MS-ISAC and the EI-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 state and local elections entities; and

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

- CIS has entered into an agreement with the federal government to provide EDR Services to certain SLTT entities.

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 EDR Services to Entity.

II. Definitions

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

B. **EDR Services**: EDR Services is comprised of the following:

1. Deployment and maintenance of an EDR software agent on Entity's identified endpoint devices, which will (a) block malicious activity at a device level if agreed to by the Entity; (b) remotely isolate compromised systems after coordination with the Entity; (c) identify threats on premise, in the cloud, or on remote systems; (d) inspect network traffic in a decrypted state on the endpoint for the limited purpose of identifying malicious activity; and (e) identify and remediate malware infections.

2. Centralized management of EDR data to allow system administration, event analysis and reporting by CIS SOC. Additionally, Entity will be able to interact with its own EDR data through the management system.

III. Consideration

Federally Funded EDR Services - Pursuant to the agreement with the federal government, CIS is providing EDR Services 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 EDR Services. Entity understands and agrees that, as a condition to commencement of EDR Services 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

The EDR Services include use of software that is licensed to CIS by a third party provider, Crowdstrike, Inc. ("Crowdstrike"). All title and ownership rights of the software shall remain with Crowdstrike.

The Customer shall own all right, title and interest in its data that is provided to CIS pursuant to this Agreement. Customer hereby grants CIS a non-exclusive, non-transferable license to access and use such data to the extent necessary to provide EDR Services under this Agreement.

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 June 30, 2021 (the "Term"), unless otherwise earlier terminated by either party or the Term is extended by agreement of the Parties.

The ability and obligation of CIS to provide these EDR Services 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

Parties disclaim all express and implied warranties with regard to the EDR Services 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 EDR Services 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's information systems, assessments and plans that relate specifically and uniquely to the vulnerability of Entity information systems, Personal Data (as defined herein below), specific vulnerabilities identified as part of the EDR Services 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 further agrees that any third party involved in providing EDR Services shall be required to protect Entity's Confidential Information to the same extent as required under this Agreement. 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 personal delivery;
3. by expedited delivery service; or
4. 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: **James Globe**
Title: **Vice President of Security Operations**
Address: **Center for Internet Security, Inc.**
31 Tech Valley Drive
East Greenbush, NY 12061-4134

Telephone Number: (518) 880-0687
E-Mail Address: james.globe@cisecurity.org

Entity Hoke County
Name: James Leach
Title: Chairman, Hoke County Board of Commissioners
Address: 227 N Main St, Raeford, North Carolina 28376
Telephone Number: 910-875-8751
E-Mail Address: gmcgougan@hokecounty.org

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 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.	**ENTITY**
By: _____	By: _____
Name: _____	Name: James Leach
Title: _____	Title: Chairman, Hoke County Board of Commissioners
Date: _____	Date: _____

Appendix A

EDR Services Responsibilities

I. **Entity Responsibilities** - Entity acknowledges and agrees that CIS's ability to perform the EDR 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 EDR 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 endpoint devices identified by Entity in the Pre-Installation Questionnaire as being included for EDR Services shall be within the scope of this Agreement. Entity will ensure the correct functioning and maintenance of the endpoint devices receiving EDR Services.

B. 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. A completed Pre-Installation Questionnaire (PIQ) to be provided to Entity by CIS, which will identify the number and types of endpoints to be monitored during the Term, including identification of the operating systems used in the endpoints. The PIQ will need to be revised whenever there is a change that would affect CIS's ability to provide the EDR Services;

2. Each endpoint device will have access to a secure Internet channel for EDR Service management and monitoring by CIS;

3. Reasonable assistance to CIS as necessary, to enable CIS to deliver and perform the EDR Services for the benefit of Entity; and

4. Accurate and up-to-date information, including the name, email, landline, mobile, and pager numbers for all designated, authorized Point of Contact(s).

C. 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 replacement of an existing endpoint device with another similar device and/or changes in operating systems for the endpoint devices that would affect CIS's ability to provide EDR Services;

2. Written notification to CIS SOC (SOC@MSISAC.ORG) at least twelve (12) hours in advance of any scheduled Internet outages affecting the endpoint devices;

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 endpoint device covered by EDR Services; and

5. Active involvement with CIS SOC to resolve any tickets requiring Entity input or action;

D. 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 shall be responsible for purchase of a commercial EDR capability provided by a third party provider, to be incorporated into the EDR Services.

B. CIS will be responsible for the deployment, management and monitoring of the EDR Services to Entity's identified endpoint devices, including provision of the link for installation of the applicable EDR agent for the

operating system of the endpoint devices, as identified by Entity in the PIQ.

C. CIS will provide the following as part of the EDR Services:

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; and

5. Ensuring that all upgrades, patches, configuration changes and signature upgrades of the EDR agent are applied to Entity's endpoint devices receiving EDR Services.

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

E. Upon termination of this Agreement, CIS shall be responsible for the cancellation of the EDR Services. Entity will be responsible for removal of the EDR software agent installed on Entity's endpoint devices.

III. Third Party Provider Terms and Conditions

Entity acknowledges and agrees that as part of providing EDR Services, CIS has contracted with the third party provider, CrowdStrike. Entity further acknowledges and agrees that in return for receipt of EDR Services, it agrees to the following terms and conditions as an end user of CrowdStrike services under this Agreement:

A. Access & Use Rights. Subject to the terms and conditions of this Agreement, Entity has a non-exclusive, non-transferable, non-sublicensable license to access and use the Products in accordance with any applicable Documentation solely for Entity's Internal Use. The Product includes a downloadable object-code component ("Software Component"); Entity may install and run multiple copies of the Software Components solely for Entity's Internal Use. Entity's access and use is limited to the quantity and the period of time specified in this Agreement.

B. Restrictions. The access and use rights do not include any rights to (i) employ or authorize any third party (other than Partner) to use or view the Offering or Documentation; (ii) alter, publicly display, translate, create derivative works of or otherwise modify an Offering; (iii) sublicense, distribute or otherwise transfer an Offering to any third party; (iv) allow third parties to access or use an Offering (except for Partner as expressly permitted herein); (v) create public Internet "links" to an Offering or "frame" or "mirror" any Offering content on any other server or wireless or Internet-

based device; (vi) reverse engineer, decompile, disassemble or otherwise attempt to derive the source code (if any) for an Offering (except to the extent that such prohibition is expressly precluded by applicable law), circumvent its functions, or attempt to gain unauthorized access to an Offering or its related systems or networks; (vii) use an Offering to circumvent the security of another party's network/information, develop malware, unauthorized surreptitious surveillance, data modification, data exfiltration, data ransom or data destruction; (viii) remove or alter any notice of proprietary right appearing on an Offering; (ix) conduct any stress tests, competitive benchmarking or analysis on, or publish any performance data of, an Offering (provided, that this does not prevent Entity from comparing the Products to other products for Entity's Internal Use); (x) use any feature of CrowdStrike APIs for any purpose other than in the performance of, and in accordance with, this Agreement; or (xi) cause, encourage or assist any third party to do any of the foregoing. Entity agrees to use an Offering in accordance with laws, rules and regulations directly applicable to Entity and acknowledges that Entity is solely responsible for determining whether a particular use of an Offering is compliant with such laws.

C. Third Party Software. CrowdStrike uses certain third party software in its Products, including what is commonly referred to as open source software. Under some of these third party licenses, CrowdStrike is required to provide Entity with notice of the license terms and attribution to the third party. See the licensing terms and attributions for such third party software that CrowdStrike uses at: https://falcon.crowdstrike.com/opensource.

D. Installation and User Accounts. For those Products requiring user accounts, only the individual person assigned to a user account may access or use the Product. Entity is liable and responsible for all actions and omissions occurring under Entity's user accounts for Offerings.

E. Ownership & Feedback. The Offerings are made available for use or licensed, not sold. CrowdStrike owns and retains all right, title and interest (including all intellectual property rights) in and to the Offerings. Any feedback or suggestions that Entity provides to CrowdStrike regarding its Offerings (e.g., bug fixes and features requests) is non-confidential and may be used by CrowdStrike for any purpose without acknowledgement or compensation, provided, Entity will not be identified publicly as the source of the feedback or suggestion.

F. Disclaimer. PARTNER, AND NOT CROWDSTRIKE, IS RESPONSIBLE FOR ANY WARRANTIES, REPRESENTATIONS, GUARANTEES, OR OBLIGATIONS TO ENTITY, INCLUDING REGARDING THE CROWDSTRIKE OFFERINGS. ENTITY ACKNOWLEDGES, UNDERSTANDS, AND AGREES THAT CROWDSTRIKE DOES NOT GUARANTEE OR WARRANT THAT IT WILL FIND, LOCATE, OR DISCOVER ALL OF ENTITY'S OR ITS AFFILIATES' SYSTEM THREATS, VULNERABILITIES, MALWARE, AND MALICIOUS SOFTWARE, AND ENTITY AND ITS AFFILIATES WILL NOT HOLD CROWDSTRIKE RESPONSIBLE THEREFOR. CROWDSTRIKE AND ITS AFFILIATES DISCLAIM ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CROWDSTRIKE AND ITS AFFILIATES AND SUPPLIERS SPECIFICALLY DISCLAIM ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGMENT WITH RESPECT TO THE OFFERINGS.

THERE IS NO WARRANTY THAT THE OFFERINGS WILL BE ERROR FREE, OR THAT THEY WILL OPERATE WITHOUT INTERRUPTION OR WILL FULFILL ANY OF ENTITY'S PARTICULAR PURPOSES OR NEEDS. THE OFFERINGS ARE NOT FAULT-TOLERANT AND ARE NOT DESIGNED OR INTENDED FOR USE IN ANY HAZARDOUS ENVIRONMENT REQUIRING FAIL-SAFE PERFORMANCE OR OPERATION. THE OFFERINGS ARE NOT FOR USE IN THE OPERATION OF AIRCRAFT NAVIGATION, NUCLEAR FACILITIES, COMMUNICATION SYSTEMS, WEAPONS SYSTEMS, DIRECT OR INDIRECT LIFE-SUPPORT SYSTEMS, AIR TRAFFIC CONTROL, OR ANY APPLICATION OR INSTALLATION WHERE FAILURE COULD RESULT IN DEATH, SEVERE PHYSICAL INJURY, OR PROPERTY DAMAGE. ENTITY AGREES THAT IT IS ENTITY'S RESPONSIBILITY TO ENSURE SAFE USE OF AN OFFERING IN SUCH APPLICATIONS AND INSTALLATIONS. CROWDSTRIKE DOES NOT WARRANT ANY THIRD PARTY PRODUCTS OR SERVICES.

G. Entity Obligations. Entity, along with its Affiliates, represents and warrants that: (i) it owns or has a right of use from a third party, and controls, directly or indirectly, all of the software, hardware and computer systems (collectively, "Systems") where the Products will be installed or that will be the subject of, or investigated during, the Offerings, (ii) to the extent required under any federal, state, or local U.S. or non-US laws (e.g., Computer Fraud and Abuse Act, 18 U.S.C. § 1030 et seq., Title III, 18 U.S.C. 2510 et seq., and the Electronic Communications Privacy Act, 18 U.S.C. § 2701 et seq.) it has authorized CrowdStrike to access the Systems and process and transmit data through the Offerings in accordance with this Agreement and as necessary to provide and perform the Offerings, (iii) it has a lawful basis in having CrowdStrike investigate the Systems, process the Customer Data and the Personal Data; (iv) that it is and will at all relevant times remain duly and effectively authorized to instruct CrowdStrike to carry out the Offerings, and (v) it has made all necessary disclosures, obtained all necessary consents and government authorizations required under applicable law to permit the processing and international transfer of Customer Data and Entity Personal Data from each Entity and Entity Affiliate, to CrowdStrike.

H. Falcon Platform. The Falcon Endpoint Protection Platform ("Falcon EPP Platform") uses a crowd-sourced environment, for the benefit of all customers, to help customers protect themselves against suspicious and potentially destructive activities. CrowdStrike's Products are designed to detect, prevent, respond to, and identify intrusions by collecting and analyzing data, including machine event data, executed scripts, code, system files, log files, dll files, login data, binary files, tasks, resource information, commands, protocol identifiers, URLs, network data, and/or other executable code and metadata. Entity, rather than CrowdStrike, determines which types of data, whether Personal Data or not, exist on its systems. Accordingly, Entity's endpoint environment is unique in configurations and naming conventions and the machine event data could potentially include Personal Data. CrowdStrike uses the data to: (i) analyze, characterize, attribute, warn of, and/or respond to threats against Entity and other customers, (ii) analyze trends and performance, (iii) improve the functionality of, and develop, CrowdStrike's products and services, and enhance cybersecurity; and (iv) permit Entity to leverage other applications that use the data, but for all of the foregoing, in a way that does not identify Entity or Entity's Personal Data to other customers. Neither Execution Profile/Metric Data nor Threat Actor Data are Entity's Confidential Information or Customer Data.

I. Processing Personal Data. Personal Data may be collected and used during the provisioning and use of the Offerings to deliver, support and improve the Offerings, comply with law, or otherwise in accordance with this Agreement. Entity authorizes CrowdStrike to collect, use, store, and transfer the Personal Data that Entity provides to CrowdStrike as contemplated in this Agreement.

J. Compliance with Applicable Laws. Both CrowdStrike and Entity agree to comply with laws directly applicable to it in the performance of this Agreement.

K. Definitions.

"CrowdStrike" shall mean CrowdStrike, Inc.

"CrowdStrike Data" shall mean the data generated by the CrowdStrike Offerings, including but not limited to, correlative and/or contextual data, and/or detections. For the avoidance of doubt, CrowdStrike Data does not include Customer Data.

"Customer Data" means the data generated by the Entity's Endpoint and collected by the Products.

"Documentation" means CrowdStrike's end-user technical documentation included in the applicable Offering.

"Endpoint" means any physical or virtual device, such as, a computer, server, laptop, desktop computer, mobile, cellular, container or virtual machine image.

"Execution Profile/Metric Data" means any machine-generated data, such as metadata derived from tasks, file execution, commands, resources, network telemetry, executable binary files, macros, scripts, and processes, that: (i) Entity provides to CrowdStrike in connection with this Agreement or (ii) is collected or discovered during the course of CrowdStrike providing Offerings, excluding any such information or data that identifies Entity or to the extent it includes Personal Data.

"Internal Use" means access or use solely for Entity's own internal information security purposes. By way of example and not limitation, Internal Use does not include access or use: (i) for the benefit of any person or entity other than Entity, or (ii) in any event, for the development of any product or service. Internal Use is limited to access and use by Entity's employees and Partner solely on Entity's behalf and for Entity's benefit.

"Entity" means a Customer of Partner that has agreed in writing to be contractually bound by these Entity Terms.

"Offerings" means, collectively, any Products or Product-Related Services.

"Partner" means Center for Internet Security, Inc.

"Personal Data" means information provided by Entity to CrowdStrike or collected by CrowdStrike from Entity used to distinguish or trace a natural person's identity, either alone or when combined with other personal or identifying information that is

linked or linkable by CrowdStrike to a specific natural person. Personal Data also includes such other information about a specific natural person to the extent that the data protection laws applicable in the jurisdictions in which such person resides define such information as Personal Data.

"Product" means any of CrowdStrike's cloud-based software or other products provided to Entity through Partner, the available accompanying API's, the CrowdStrike Data, any Documentation.

"Product-Related Services" means, collectively, (i) Falcon OverWatch, (ii) Falcon Complete Team, (iii) the technical support services for certain Products provided by CrowdStrike, (iv) training, and (v) any other CrowdStrike services provided or sold with Products.

"Threat Actor Data" means any malware, spyware, virus, worm, Trojan horse, or other potentially malicious or harmful code or files, URLs, DNS data, network telemetry, commands, processes or techniques, metadata, or other information or data, in each case that is potentially related to unauthorized third parties associated therewith and that is collected or discovered during the course of CrowdStrike providing Offerings, excluding any such information or data that identifies Entity or to the extent that it includes Personal Data.

ENTITY CERTIFICATION

On behalf of Hoke County Board of Elections ("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 ___ day of _____, 20__.

_____

Name: James Leach

Title: