Cybersecurity Services Agreement

This Agreement between the **Indiana Secretary of State ("The State"), Carahsoft Technology Corp., FireEye, Inc.**, and **FireEye, Inc., DBA "Mandiant" ("The Contractors")** and _____ **County ("The County")** is entered pursuant to the following terms and conditions.

Whereas, Securing state and county election infrastructure including associated information technology systems and networks is a matter of great public importance.

Whereas, The State has undertaken to secure an array of coordinated cyber and IT security services provided by **The Contractors**, available to **The County** pursuant to **This Agreement**.

Whereas, terms of IT and cyber security services available to **The County** from **FireEye, Inc.**, are provided in **Attachment A**, a procurement by **The State,** funding for which has been provided by 2018 HAVA Election Security Grant Funds.

Whereas, The State has contracted for certain quantity of IT and cyber security ***Incident Response Services*** from **FireEye, Inc., DBA "Mandiant"** as provided in **Attachment B**, funding for which has been provided by 2018 HAVA Election Security Grant Funds.

Whereas, The State will endeavor to make ***Incident Response Services*** available to **The County** on application, based on priority, severity of need, and resource availability, at the sole discretion of **The State**.

Whereas, neither **The State** nor **The Contractors** will levy or assess any charge on **The County** for services detailed in **Attachment A.** Optional Utilization of ***Incident Response Services*** by **The County** may obligate **The County** to incidental expenses as detailed in **Attachment B**.

Whereas, The County acknowledges that in order to fully benefit from the services detailed in **This Agreement,** cooperation, coordination, effort, and optional incidental expenses on the part of **The County** will be required.

Whereas, the period of time services detailed in **Attachment A** and optional services detailed in **Attachment B** will be available to **The County** pursuant to **This Agreement** will be limited to the term of the agreement between **The State** and **The Contractors**, such term beginning approximately September 1, 2019 and ending December 31, 2022.

1. Responsibilities of The County. Specific responsibilities of **The County** are detailed in **Attachment C.**

2. Responsibilities of The State. Specific responsibilities of **The State** are detailed in **Attachment D.**

P1/22

3. Term. This Agreement shall commence on the date approved by the last signatory and shall end on December 31, 2022.

4. Definitions.

5. Confidential Non Public Infrastructure Security Information and Trade Secrets. **The County** acknowledges that pursuant to **This Agreement, The State** may provide or produce information designated as ***"Non Public Infrastructure Security Information"*** and **The Contractors** may provide or produce information designated as ***"Trade Secret"***. **The County** acknowledges and agrees that information designated as ***"Non Public Infrastructure Security Information"*** or ***"Trade Secret"*** received pursuant to **This Agreement** will be handled and maintained in a secure and confidential manner and in accord with the *Indiana Public Records Act* (IC 5-14-3) ***not*** provided to third parties or made available for public access without written authorization from **The State** or **The Contractors** as applicable.

6. Federal Funding; Audits; Maintenance of Records. The County and its contractors, if any, shall maintain all books, documents, papers, accounting records, and other evidence pertaining to services received under **This Agreement. The County** acknowledges that it may be required to submit to federal or state audit of services received or funds paid on its behalf. If it is determined that **The County** is a "sub recipient", and if required by applicable provisions of 2 C.F.R. 200 (Uniform Administrative Requirements, Cost Principles, and Audit Requirements), **The County** shall submit to a financial and compliance audit, which complies with 2 C.F.R. 200.500 *et seq*.

7. HIPAA Compliance. If This Agreement involves services, activities or products subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), **The County** covenants that it will appropriately safeguard Protected Health Information (defined in 45 CFR 160.103), and agrees that it is subject to, and shall comply with, the provisions of 45 CFR 164 Subpart E regarding use and disclosure of Protected Health Information.

8. Other Federally Required Contract Provisions. Services provided **The County** pursuant to This Agreement will be paid for using federal funds. **The County** acknowledges it may be responsible for compliance with requirements imposed by the federal government such as those set forth in **Attachment E. The County** will determine its need to comply with federal contract provisions.

9. Assignment; Successors. The County binds its successors and assignees to all the terms and conditions of **This Agreement.**

10. Assignment of Antitrust Claims. As part of the consideration for **This Agreement, The County** assigns to **The State** all right, title and interest in and to any claims **The County** may acquire, under state or federal antitrust laws relating to the products or services which are the subject of this **This Agreement**.

P 7/22

10. Changes in Services. **The County** will not order, commence or bind **The State** or **The Contractors** to any additional services, work or expenses, or change the scope of the services provided under **This Agreement** without written authorization by **The State**. The County shall make no claim for associated expenses or effort in the absence of a prior written approval and amendment executed by all signatories hereto. **This Agreement** may only be amended, supplemented or modified by a written document executed in the same manner as **This Agreement**.

11. Funding Cancellation When **The State** or the Director of the State Budget Agency makes a written determination that funds are not appropriated or otherwise available to support continuation of performance of **This Agreement, This Agreement** shall be canceled. A determination by the Director of State Budget Agency that funds are not available or otherwise appropriated to support continuation of performance shall be final and conclusive.

12. Governing Law. **This Agreement** shall be governed, construed, and enforced in accordance with the laws of the State of Indiana, without regard to its conflict of laws rules. Suit, if any, must be brought in the State of Indiana.

13. Indemnification. **The County** and **The State** shall each be solely responsible for their own acts or omissions or acts or omissions of their employees, officials, agents or contractors. Each of the parties to **This Agreement** is a governmental entity for the purposes of the Indiana Tort Claims Act ("ITCA"), IC 34-13-3 *et seq*. Accordingly, neither party shall be required to indemnify the other, and each party shall bear its own risk of loss in connection with **This Agreement**.

14. Insurance. **The State** is prohibited by IC § 4-13-1-17(a) from purchasing insurance to cover loss or damage to property and is prohibited by IC § 34-13-3-20(c) from purchasing insurance to cover the liability of **The State** or its employees. **The County** shall keep in force during the period of This Agreement such insurance as it deems necessary to protect its interests.

15. Merger & Modification. **This Agreement** constitutes the entire agreement between the parties. No understandings, agreements, or representations, oral or written, not specified within **This Agreement** will be valid provisions of **This Agreement**. **This Agreement** may not be modified, supplemented, or amended, except by written agreement signed by all necessary parties.

16. Notice to Parties. Whenever any notice, statement or other communication is required pursuant to **This Agreement**, it will be sent by first class U.S. mail service or established commercial courier service to the following addresses, unless otherwise specifically advised. ***Note: See Attachment C "Responsibilities of the County" for notification of IT technical issues, security incidents, or for customer support.***

A. Notices to **The State** shall be sent to:

Jerold Bonnet, General Counsel
Office of the Indiana Secretary of State
200 W. Washington St. Room 201
Indianapolis, IN 46204

B. Notices to **The County** shall be sent to:

17. Order of Precedence; Incorporation by Reference. Any inconsistency or ambiguity in **This Agreement** shall be resolved by giving precedence in the following order: (1) **This Agreement**, (2) attachments prepared by **The State**, (3) attachments prepared by **The Contractors**. All attachments, and all documents referred to in this paragraph, are hereby incorporated fully by reference.

18. Severability. The invalidity of any section, subsection, clause or provision of **This Agreement** shall not affect the validity of the remaining sections, subsections, clauses or provisions of **This Agreement**.

19. Termination for Convenience. **This Agreement** may be terminated, in whole or in part, by **The State**, which for the purpose of this paragraph shall include IDOA and the State Budget Agency, whenever, for any reason, **The State** determines that such termination is in its best interest. For the purposes of this paragraph, the parties stipulate and agree that IDOA shall be deemed to be a party to **This Agreement** with authority to terminate the same for convenience when such termination is determined by the Commissioner of IDOA to be in the best interests of the State.

21. No Warranties. With respect to **This Agreement** and services provided by **The Contractors, The State** makes no warranties of any kind. **The State** disclaims responsibility for any representations or any warranties express or implied made by **The Contractors** or contained in any part of **This Agreement** or attachments hereto.

22. Waiver of Rights. No right or responsibility conferred on either party under **This Agreement** shall be deemed waived, and no breach of **This Agreement** excused, unless such waiver is in writing and signed by the party claimed to have waived such right. Neither **The State's** review, approval or acceptance of, nor payment for, services provided pursuant to **This Agreement** shall be construed to operate as a waiver of any rights or responsibilities under **This Agreement.**

11. Authority to Bind Contractor. The signatory for **The County** represents that he/she has been duly authorized to execute **This Agreement** on behalf of **The County** and has obtained all

PY/22

necessary or applicable approvals to make **This Agreement** fully binding upon **The County** when his/her signature is affixed, and accepted by **The State**.

The remainder of this page is intentionally blank.

P5/22

Non-Collusion and Acceptance

The undersigned attests, subject to the penalties for perjury, that the undersigned is **The County** or other party to **This Agreement**, or that the undersigned is the properly authorized representative, agent, member or officer of **The County** or other party to **This Agreement**. Further, to the undersigned's knowledge, neither the undersigned nor any other member, employee, representative, agent or officer of **The County**, directly or indirectly, has entered into or been offered any sum of money or other consideration for the execution of **This Agreement** other than that which appears upon the face hereof. **Furthermore, if the undersigned has knowledge that a state officer, employee, or special state appointee, as those terms are defined in IC § 4-2-6-1, has a financial interest in This Agreement, The County or other party attests to compliance with the disclosure requirements in IC § 4-2-6-10.5.**

In Witness Whereof, The County and **The State** have, through their duly authorized representatives, entered into **This Agreement**. The parties, having read and understood the foregoing terms of **This Agreement** do by their respective signatures dated below agree to the terms thereof.

Vigo **County [The Contractor]**

By: Brad Anderson, President Vigo Co. Commissioners

Name and Title, Printed

Date: 12-10-2019

Indiana Secretary of State [The State]

By: _____
Brandon Clifton, Deputy Secretary of State

Date: _____

List of Attachments:

Attachment A – IT and Cyber Security Services SOW - FireEye Inc. SOW

Attachment B –Incident Response Services SOW– FireEye, Inc., DBA "Mandiant"

Attachment C – Responsibilities of The County

Attachment D – Responsibilities of The State

Attachment E – Federal Funds Recipient Requirements

FIREEYE

Attachment A

IT and Cyber Security Services available to Counties

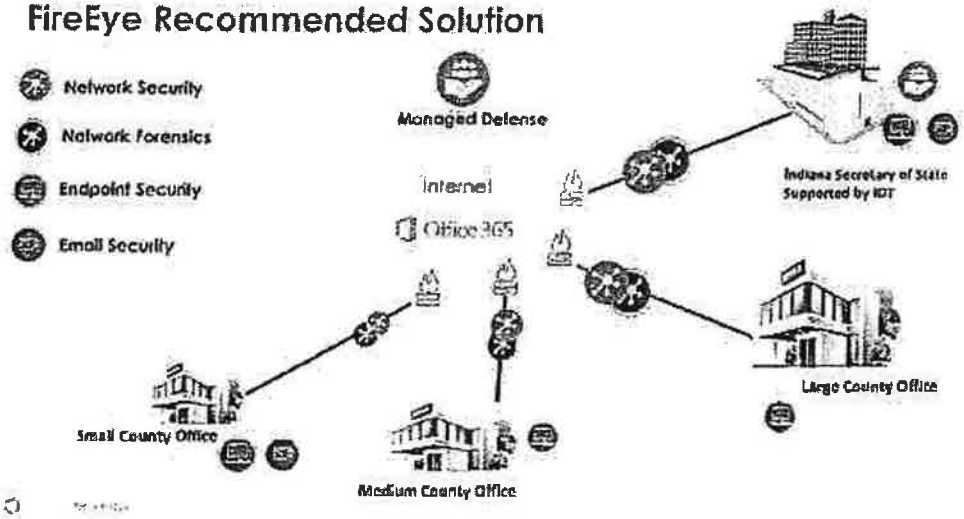
STATEMENT OF WORK – US DEPLOYMENT

This Statement of Work ("SOW") is effective as of the date of Customer's purchase order_____ to the applicable reseller/distributor: Carahsoft Technology Corp. ("Carahsoft"), for the services described in this SOW ("SOW Effective Date"). FireEye, Inc., ("FireEye") will provide the Services described in this SOW to the INDIANA SECRETARY OF STATE ("Customer"). This SOW is governed by the Carahsoft - Customer agreement and the Carahsoft-FireEye Distributor Agreement; the latter incorporating terms at https://www.fireeeye.com/company/legal for the applicable FireEye Offerings specified in the above-referenced Customer Carahsoft purchase order.

1 DESCRIPTION OF SERVICES:

FireEye will plan, deploy, and integrate the proposed FireEye Security solution to the 92 in-scope State of Indiana County Election Office networks according to FireEye's best practices methodology designed to achieve the best use of the technology. The proposed solution consists of:

- FireEye Central Manager (one cloud management instance across all County Office networks)
- FireEye EndPoint Security (one cloud management console instance across all County Office networks with local software agents deployed on endpoints within each County Office network)
- FireEye Network Security (one physical appliance per County Office network)
- (Optional) FireEye Email Threat Prevention (one cloud management instance across all County Office networks with O365 integration for each County Office email domain)
- FireEye Managed Defense Service (above systems will be provisioned for FireEye Managed Defense Service to provide on-going advanced threat protection for County Office networks).



P7/22

FIREEYE

This project will consist of the following activities:

Project Management

During Deployment:

- FireEye will provide a designated Project Manager for the duration of the installation through the Planning and Design, Installation and Configuration, Configuration and Deployment Testing, and Knowledge Transfer and Operational Handoff phases. The FireEye Project Manager will function as a single point of contact for the FireEye deployment team and will work closely with the Customer Project Manager to schedule and manage the deployment.

Post Deployment:

- FireEye will provide a designated Project Manager for the duration of the SOW following the phases listed above. The FireEye Project Manager will coordinate with the Customer and provide project oversight to help ensure deliverables meet mutually agreed timelines and SOW specifications.

Planning and Design

FireEye will participate in planning to cover the following:

- Review program objectives, high-level list of activities, and milestones
- Develop detailed project plan listing the activities, dependencies, duration and resources for the deployment activities
- Review County Office network architecture diagrams, change control processes, other business processes, and security goals to determine the appropriate design and configuration plan for the FireEye solution
- Develop policy to be applied across all FireEye Endpoint Security agents and reach agreement on the policy with Customer
- Develop common configuration to be applied for each FireEye Network Security appliance and reach agreement on the configuration with Customer
- Develop configuration to be applied for the FireEye Email Security solution
- Work with Customer PM to gather information from each County Office needed for planning each deployment
- Work with Customer PM to plan the deployment for each County Office

Installation and Configuration

To ensure successful installation and configuration, FireEye will assist Customer's EOC with the deployment of the FireEye solution components in their networks. The installation will consist of an initial set up approximately eight pilot County Office networks. Installation of additional County Office networks will be scheduled after the pilot set is complete and lessons learned are incorporated into the plans for remaining deployments. All components for a given County Office /network are to be installed within a single onsite visit up to two days in length.

The deployment services will consist of a combination of tasks and knowledge transfer, including:

FireEye Central Manager (cloud instance)

- Provision one FireEye Central Manager (CM) cloud instance to be shared across all COUNTY offices
- Validate access to cloud CM instance
- Configure users and permission sets
- Configure notification settings

FIREEYE

FireEye EndPoint Security (cloud instance with local agents)

- Provision one FireEye Endpoint Security management console cloud instance to be shared across all COUNTY offices
- Configure the agreed upon FireEye EndPoint Security policy to be applied across in-scope endpoints
- Configure the FireEye Endpoint Security management console per FireEye recommended best practices and Customer's requirements
- Integrate the FireEye Endpoint Security management console with the FireEye Central Manager
- Integrate the FireEye Endpoint Security management console with the FireEye Managed Defense service
- For each County Office network, deploy the FireEye Endpoint Security agent on up to five endpoints and verify connectivity and network communications with the Endpoint Security management console
- For each County Office network, provide the FireEye Endpoing Security agent deployment package and instructions for deploying Endpoint Security agents on up to 100 endpoints for devices running supported versions of Microsoft Windows, Linux, or macOS

FireEye Network Security (physical appliance)

- For each County Office network, deploy one FireEye Network Security physical appliance. For County Office networks where a customer resource is not available to rack and cable the appliance, FireEye will rack and cable the appliance with Customer's guidance on rack location, physical network connections, etc.
- Configure network settings for management port and IPMI port (IP address, subnet mask, and gateway)
- Verify network connectivity for management port and remote accessibility
- Apply latest operating system and security content updates
- Configure network monitoring ports for inline or SPAN/TAP mode per Customer requirements
- Configure the FireEye Network Security appliance according to the common configuration
- Review network traffic statistics for capture ports to verify deployment and configuration
- Integrate the FireEye Network Security appliance with the FireEye Central Manager
- Integrate the FireEye Network Security management console with the FireEye Managed Defense service
- Validate connectivity to Managed Defense
- Test alerting capability and verify alert flow

Optional – Email Threat Prevention (ETP)

- Provision one FireEye Email Security management console cloud instance to be shared across all County Office
- Integrate FireEye Email Security with Customer's O365 email solution
- Apply the agreed upon configuration for Email Security to detect and prevent email-based threats
- Customer will perform MX record changes to support inline operation of ETP
- Integrate the FireEye Email Security management console with the FireEye Central Manager
- Integrate FireEye Email Security with the FireEye Managed Defense service
- Validate connectivity to Managed Defense

FIREEYE

Managed Defense Integration

- Ensure all components are integrated with FireEye's Managed Defense
- Validate Managed Defense access for all components
- Verify Managed Defense reporting and alerting

Configuration and Deployment Testing

FireEye will review the architecture, processes, testing, and steps required to validate the proper function and configuration of the FireEye solution within Customer's environment. The mutually agreed upon test plan will include connectivity, configuration, and operational and integration test use cases. FireEye will work with Customer to test the appropriate configurations throughout the deployment to meet their business requirements.

Knowledge Transfer and Operational Handoff

FireEye will provide up to three knowledge transfer sessions for designated points of contact for Customer Network / Security administrators to cover the installation process, configurations for each product type, and on-going administration and responsibilities for the FireEye security solution. Knowledge transfer sessions will include Managed Defense roles and responsibilities and the operational handoff to Managed Defense.

FireEye Security Engineer – First Year Post Implementation Support and Management

A FireEye Security Engineer will work as an integral part of Customer's team onsite and remotely to sustain Customer's FireEye solution. Tasks that may be performed by the FireEye Security Engineer include:

- Perform regular status checks on the FireEye solution to ensure the FireEye Network Security, FireEye Endpoint Security, and FireEye Central Manager components are up to date on patches, security content, and guest images and perform updates as needed
- Perform regular health checks on the FireEye solution to ensure components are operating properly and within the expected performance range
- Document health and status checks and any updates made to the FireEye products
- Provide guidance on and assist with additional FireEye appliance deployments as needed
- Time permitting during the FireEye Security Engineer's normal working hours, assist Indiana Secretary of State in following-up on published Managed Defense Investigations within Customer's networks, up to ten investigations per day. This task would consist of attributing the investigation to a county based on affected hostname for an endpoint alert or network sensor name for a network alert and communicating the alert to the county POC
- Provide weekly written status updates

Cyber Security Analyst

FireEye will provide an on-site resource (Consultant) to support a twelve (12) month period to the executive leadership of Customer to help develop and implement remediation strategies associated with the proposed Security solution activities and initiatives. Consultant will be responsible for interfacing with FireEye Managed Defense resources on behalf of Customer in the event that Rapid Response is required in order to ensure actions are executed in a timely and appropriate manner and addressing or coordinating remediation activities with the counties under the purview of Customer, if needed. Consultant may provide professional services to perform proactive breach detection (hunting) and incident triage. Consultant will work side-by-side with the Security Operations Center (SOC) staff, or Customer Security staff, to assist with

FIREEYE

detection, response and containment, at the discretion of SOC leadership, and can also lead Incident Response efforts as required. Consultant will also be available for special projects and will continue efforts to mature the SOC staff by providing on-the-job training during day-to-day operations.

Digital Threat Assessments

FireEye will provide six (6) one-time assessments over a thirty-six (36) month period, each assessment will be conducted over thirty (30) days (unless otherwise agreed in writing) (the "Assessment Period"), through which FireEye will search for Keywords to uncover evidence of threat actor activity related to these Keywords. Prior to each Assessment Period, FireEye will meet with the Customer to determine Keywords and conduct a brief quality assurance test on the keywords. FireEye will conduct at least one meeting during each Assessment Period to inform Customer on progress and answer questions about the assessment. Following the conclusion of each Assessment Period, FireEye will provide Customer with one (1) Deliverable report summarizing each applicable assessment findings.

2 DELIVERABLES:

The Deliverables to be produced under this SOW are as follows:

- FireEye Implementation Planning Document
- FireEye Solution Design
- Completed FireEye Deployment Checklist for each County Office network including deployment test results
- FireEye Deployment Report
- Weekly Status Updates
- Six (6) individual Digital Threat Assessment Reports

3 TERM AND LEVEL OF EFFORT FOR SERVICES:

Services will begin on a mutually agreeable date after the SOW Effective Date; and, except for the Digital Threat Assessment Period (36 months), are expected to take one year to complete (including approximately four months for deployment services and project management services as described above and eight months for post deployment security engineer services as described above). The Deliverables listed in this SOW will be provided during the SOW engagement. Unless otherwise agreed, Services (including FireEye Security Engineer and Cyber Security Analyst services) will be delivered during standard business hours Monday to Friday, excluding U.S. government holidays and scheduled time off. Except for the Digital Threat Assessment Period, all other SOW Services must be used within one year of the SOW Effective Date; and any unused Services expire one year after the SOW Effective Date.

4 LOCATION OF PERFORMANCE OF SERVICES:

FireEye will use a blend of onsite and offsite resources to deliver the Services set forth in this SOW.

5 FEES AND EXPENSES:

In consideration of the Services to be provided, Customer agrees to pre-pay the Services Fixed Fees as quoted to the Customer by the applicable reseller. Pre-paid Services Fixed Fees will be invoiced on or about the SOW Effective Date and Customer will pay in accordance to the terms of the Agreement (Upfront Billing). Pre-paid Services Fixed Fees are non-cancellable and non-refundable. Quoted Services Fixed Fees include travel expenses for the deployment services specified above for one onsite visit up to two days in length per County Office and for travel to County Offices by the FireEye Security Engineer and/or the Cyber Security Analyst, if required for the performance of the post deployment services.

FIREEYE

6 CUSTOMER RESPONSIBILITIES:

The tasks for which Customer is responsible under this SOW are:

- Customer will appoint a primary Project Manager and a secondary Project Manager for FireEye to work with throughout the engagement to schedule deployment activities, knowledge transfer sessions, weekly updates, and follow-up discussions as necessary. Customer Project Manager will act as a single point of contact for Customer throughout the engagement and will facilitate Customer action items to prevent delays in the agreed upon deployment schedule.
- For work performed at Customer's facilities (e.g. each County Office /network), Customer will provide access to the necessary systems, workspace, and Internet access for FireEye's employees including necessary access tokens and ID badges as required for this project.
- For County Office networks where Customer has onsite staff to rack and cable the FireEye appliances, Customer will ensure all FireEye appliances are unboxed, racked, and cabled prior to FireEye's arrival onsite for the installation.
- For County Office networks where Customer does not have onsite staff to rack and cable the FireEye appliances, Customer will inspect FireEye appliances for any sign of physical damage due to shipping and will alert FireEye of such damage prior to FireEye's arrival onsite for the installation. Customer will provide detailed instructions on the placement of the FireEye appliances in the network rack and on the cabling of the appliances. Customer will provide power cables compatible with the available rack, a power source with two outlets for each appliance, and the appropriate network cables for monitoring and management ports for each FireEye appliance.
- Customer will deploy FireEye Endpoint Security agents to in-scope endpoints beyond the initial five endpoints within each County Office Office/network that are deployed by FireEye. FireEye will provide the Endpoint Security agent installation package and instructions.
- Throughout the course of this engagement, Customer will make available key individuals within its organization and information that can best help plan and execute the Services described in this SOW, including:
    - Customer staff members will be available to provide infrastructure support during the installation / configuration
    - Customer will provide FireEye with relevant network diagrams and other relevant documentation to facilitate proper deployment of FireEye systems
    - Customer will make available staff members for knowledge transfer during the scheduled services delivery period

7 CONTACT INFORMATION:

Customer will provide contact information to FireEye for those Customer personnel who are designated as Customer's points of contact for the Services.

P12/22

Attachment B

Optional Incident Response Services

MANDIANT

Statement of Work SOS#

This Statement of Work ("SOW") is effective as of the date of Customer's purchase order 1959569-02 to the applicable reseller/distributor: Carahsoft Technology Corp. ("Carahsoft"), for the Services described in this SOW ("SOW Effective Date"). FireEye, Inc., ("FireEye") will provide the Services described in this SOW to the INDIANA SECRETARY OF STATE ("Customer"). This SOW is governed by the Carahsoft - Customer agreement and the Carahsoft-FireEye Distributor Agreement; the latter incorporating terms at https://www.fireeeye.com/company/legal for the applicable FireEye Offerings specified in the above-referenced Customer - Carahsoft purchase order.

Mandiant agrees to provide services ("Services") as set forth below. The Services will consist of the following:

Mandiant agrees to provide incident response services ("Incident Response Services") during the forty (40) month period from the SOW Effective Date (the "Covered Period"). Each request for Incident Response Services that is confirmed under this SOW, will consume a minimum of forty (40) hours. During the Covered Period Mandiant will provide Incident Response Services as requested by Customer in the following areas:

- Computer security incident response support
- Digital forensics, log, and malware analysis support
- Incident remediation assistance

Upon SOW execution, Customer will receive a welcome letter that describes the Mandiant Incident Response Service Declaration Process, 24/7 contact information and email address for requesting Incident Response Services. Customer is provided access to Mandiant's toll-free hotline, which is available twenty-four (24) hours a day and seven (7) days a week.

Following Customer's request for Incident Response Services, Mandiant will engage with Customer to determine if Incident Response Services are required or if Mandiant is able to effectively assist based on the situation. Mandiant will respond to Customer's request within a maximum of four (4) hours following the initial request. If Mandiant and Customer agree that Incident Response Services are necessary, Mandiant will assign a Mandiant Incident Response Lead ("IR Lead") within twenty-four (24) hours of the Customer's request for Incident Response Services. The time frames to respond to Customer's request for Incident Response Services and assign an IR Lead, as described above, are collectively called the "IR Service Levels."

Upon engagement for Incident Response Services as described above, the IR Lead will determine the appropriate next steps with Customer. This may include one of the following common scenarios: 1) Customer provides Mandiant evidence (e.g., logs, malware samples, forensic images or live response datasets) to analyze, 2) Customer leverages Mandiant's endpoint technology, either remote or on premise, to enable Mandiant to perform analysis of a system of interest or a large number of systems. During this discussion, Customer and Mandiant will determine the appropriate technology stack, if any, required to complete the analysis.

If Mandiant and Customer determine that the requested Incident Response Services can be performed using Mandiant's technology stack, Mandiant will provide the required components to Customer for installation on the Customer endpoints

to be analyzed (each, an "Endpoint"). Mandiant may also provide network equipment to Customer for installation to facilitate Mandiant's network monitoring procedures.

Customer acknowledges that Mandiant may use other tools, including cloud-based analytics tools and cloud-email monitoring tools, in the course of performing Services, and agrees that Mandiant may use all such tools in its discretion. Customer will cooperate with Mandiant to facilitate Mandiant's use of any such tools. Any charges for such tools are set forth in the Technology Fees section of this SOW (Section 5) or will be agreed upon between the parties jointly in writing.

Mandiant and Customer will coordinate the delivery of the Incident Response Preparedness Service one time during the first twelve (12) months of the SOW Covered Period. This service is an essential part of the Incident Response Retainer Service and should be completed as early as possible to ensure Mandiant's ability to respond effectively to your Incident Response needs. The objective is to complete this activity within ninety (90) days from the SOW Effective Date. The Incident Response Preparedness Service is designed to provide Mandiant with an understanding of Customer's current capabilities to support a Mandiant Incident Response engagement. This activity will be conducted at a single Customer location and will include the following:

- Mandiant will conduct up to four (4) workshops with key managers, team members, and technical leaders within the organization to better understand Customer's environment, ability to quickly deploy Mandiant technology, and to immediately provide Mandiant first responders with the critical information. These workshops will review existing Customer incident response plans, technologies deployed and log sources in place to detect, analyze, and respond to a breach.
- Mandiant will provide recommendations on necessary play books for Customer to develop and maintain, to ensure:
  - Proper procedures and points of contact are known for technology (software and hardware) deployment.
  - Customer can quickly provide critical information to enable the incident response team to investigate a breach.

In addition to the Mandiant Services described in Section 1.1 and 1.2 of this SOW, during the Covered Period, Mandiant may provide additional consulting services on a per-request basis, as described below. The activities to be performed may be more explicitly defined and approved as mutually agreed upon "Work Orders" under this SOW or, in some cases where a Work Order is not necessary, may be described on informational quotes accepted by Customer. For purposes of clarity, this SOW does not obligate Customer to any additional fees unless and until both parties execute a Work Order as set forth below, or, if no Work Order is necessary, until the Customer has accepted FireEye's informational quote. Customer's receipt of Services will constitute acceptance of the quote. The following services can be requested via a Work Order:

- Mandiant Strategic Consulting Services
  - Security Program Assessment
  - Security Program Transformation
  - Response Readiness Assessments
  - Table Top Exercises
- Mandiant Technical Services
  - Compromise Assessments
  - Investigative Support, Forensics, Litigation Support, and Advisory Services (other than Incident Response Services)
- Mandiant Proactive Services
  - Vulnerability Assessments
  - Penetration Testing
  - Red Team Assessments
  - Red Team Operations

P14/22

For each Work Order under this SOW, Mandiant and Customer will agree on a defined scope and any Deliverables that are unique to each Work Order, and the number of hours to be drawn from the total purchased as set forth in Section 4. Each Work Order will be a separate document governed by this SOW.

Work Order Process

During the Covered Period, Customer may request Services under this Section 1.3 of this SOW, and if mutually agreed, Mandiant and Customer may enter into a separate, mutually agreed-upon work order ("Work Order") with respect to such Services. All such Work Orders will incorporate and be governed by the terms of the Agreement and this SOW.

Each Work Order under this SOW will contain the following sections:

- Detailed description of requested work
- Estimate of requested effort including hours and duration
- Work Order Deliverables
- Estimated expenses and fees (including technology fees, if applicable)

Process for execution of a Work Order:

- Customer will request a Work Order estimate from Mandiant
- Mandiant will develop at no cost to Customer a Work Order containing the sections as described above.
- Mandiant will then send the Work Order to the Customer for review and approvals.
- A Work Order shall be deemed accepted only if executed by authorized signatories of each party.

All work under specific Work Orders will be performed in accordance with the hourly rate quoted by the applicable reseller. Services under a Work Order will not commence until the Work Order has been executed. Customer will pay all invoices as agreed between Customer and the applicable reseller. Unless otherwise agreed upon in the Work Order, invoices for the fees and expenses will be issued on a monthly basis in arrears. Actual expenses will be invoiced as set forth in Section 6 and technology fees will be invoiced as set forth in Section 5.

Below are Deliverables that may be produced. Additional Deliverables may be defined as part of Work Orders as described in Section 1.3.

Any other reports (including intelligence reports), presentations, materials or other written information provided by Mandiant as a result of the Services are Mandiant IP and will not be considered "Deliverables" as defined in the Agreement.

The following Deliverables may be produced for Incident Response Services:

- – During a declared Incident Response engagement, Mandiant will provide weekly status reporting that will summarize activities completed, key engagement statistics, issues requiring attention and plans for the next reporting period.
- – Upon completion of any declared Incident Response engagement, Mandiant will provide a detailed final report covering the engagement activities, results and recommendations for remediation in a written detailed technical document.

P15/22

– Upon completion of any declared Incident Response Service engagement and as required to inform senior executives or board level members, Mandiant will provide an executive brief that summarizes engagement results and recommendations in executive format.

– Upon completion of the Incident Response Preparedness Service, Mandiant will provide an executive-level brief detailing Mandiant's recommendations to improve Customer's incident preparedness capabilities. The report will include an inventory of existing Customer incident response plans, technologies deployed, and log sources in place to detect, analyze, and respond to a breach.

All parties will mutually agree to the scheduling of Services under this SOW and each Work Order, as applicable. Any Services described in Section 1.3 must commence within the Covered Period, and must be requested no later than forty-five (45) days prior to the end of the Covered Period to allow for scheduling so that Services may commence prior to the end of the Covered Period.

Customer agrees to pay the fees incurred as quoted to Customer by the applicable reseller and any applicable expenses incurred. Customer will pay the pre-paid fees quoted by the applicable reseller ("Pre-Paid Fees"), which will include fees for the IR Service Levels, Incident Preparedness Service and 570 Pre-Paid Hours ("Pre-Paid Hours"). Pre-Paid Fees are non-cancelable and non-refundable. Any hours incurred for Services that exceed the Pre-Paid Hours ("Additional Hours") will be invoiced monthly in arrears, as they are incurred, according to the Additional Hours rate quoted by the reseller. Pre-Paid Fees do not include Additional Hours, travel time, technology fees, expenses, or long-term evidence storage. All such fees and costs will be invoiced monthly in arrears, as they are incurred.

When Customer has requested Services under this SOW and Mandiant has been engaged, Mandiant and Customer will determine the appropriate technology components required. In addition to professional services fees in Section 4, Customer agrees to pay technology fees in support of Services as quoted to Customer by the applicable reseller.

Customer shall reimburse Mandiant for the following expense categories that are directly attributable to work performed under this SOW:

- Travel and living expenses.
- Mileage in company or personal vehicles
- Computer storage media.
- Postage and courier services.
- Shipping, freight, import duties, and tariffs.
- Printing, reproduction, and binding.
- Any other expenses resulting from the work performed under this SOW.

Upon request, Mandiant will provide electronic copies of expense receipts for all expense related items greater than $25. Expenses will be invoiced monthly in arrears as incurred.

P16/22

1. Mandiant will provide Deliverables to Customer throughout this engagement. Draft Deliverables are considered final upon confirmation from Customer (written or oral) or ten (10) business days after their submission date from Mandiant to Customer, whichever is earlier.

2. When Mandiant's personnel are performing Services on site at Customer's premises, Customer will allocate appropriate working space and physical access for all Mandiant assigned personnel. To accomplish the work described in this SOW or a Work Order, Mandiant may use both onsite or off-site personnel, depending on the tasks desired by Customer and agreed upon by Mandiant.

3. Customer will make available key individuals that can best help plan operations around security event monitoring, analysis, threat intelligence, and incident response.

4. Estimated professional fees do not include any hardware, software, licensing, maintenance, or support costs of any Mandiant or other third-party product or service suggested by Mandiant as we conduct the activities outlined within this SOW.

5. All parties will mutually agree upon any changes to this SOW in writing.

Customer will provide Mandiant with points of contact information in the following table:

Technical Point of Contact	
Name:	
Title:	
Email:	
Phone:	
Street:	
City:	
State:	
Zip:	

The below terms will apply to any Proactive Service (including penetration testing and red team engagements) requested under this SOW or any Work Orders.

1. As a part of any penetration testing that may be part of this SOW, Mandiant may, among other things, (a) scan Customer's network and systems for ports, services and other entry points that can be exploited; and (b) probe those entry points in an effort to gain access to Customer's network and systems in an effort to determine the severity of the vulnerability.

2. CUSTOMER UNDERSTANDS THAT, ALTHOUGH MANDIANT TAKES PRECAUTIONS TO AVOID DAMAGE TO CUSTOMER'S NETWORK AND SYSTEMS, DISRUPTIONS, OUTAGES AND/OR DATA LOSS MAY OCCUR AS A RESULT OF ANY PENETRATION TESTING. Customer represents and warrants that all systems

on its network or otherwise accessible during the penetration test have been backed up, and that any data loss or other damage caused by the penetration testing can be easily and quickly reversed.

3. If appropriate, Customer will provide to Mandiant certain information required for performing its tests, including a description and location (e.g., an IP address) of the systems and networks to be tested. Customer represents and warrants that all information provided is true and accurate and that Customer owns or is authorized to represent the owners of the systems and networks described in connection with the penetration testing.

4. If appropriate, Customer may inform all or a selected group of its employees, contractors, and other third parties about any penetration testing to be undertaken by Mandiant. In the event that Customer decides not to inform anyone of the penetration testing, Customer understands that people may spend time and money on behalf of Customer in detecting, blocking, investigating or responding to activities of Mandiant. IN LIGHT OF THE POSSIBILITY THAT SUCH ACTIONS MAY BE TAKEN AND EXPENDITURES MAY OCCUR, CUSTOMER SHOULD CONSULT WITH CUSTOMER'S LEGAL COUNSEL AND/OR A MEMBER OF EXECUTIVE MANAGEMENT PRIOR TO ANY SUCH ZERO KNOWLEDGE ENGAGEMENTS. Customer may also want to consider contacting such third-party service providers as Customer's telecommunications carrier to alert them to the testing.

5. If appropriate, user data contained on systems that are tested may be accessible to Mandiant and Mandiant may download portions of such data (e.g., as proof of access).

6. If appropriate, at any point during the testing, either party may pause or stop the test. Should the testing be terminated, a rationale for such termination shall be provided by the party requesting such termination and such rationale shall be clearly documented.

P 8/22

Attachment C

Responsibilities of the County

The tasks for which **The County** is responsible under **This Agreement** are:

- **The County** will provide and authorize an appropriate primary representative and points of contact for coordination, scheduling, technical information, deployment and local management of the IT and cyber security services as detailed in **Attachment A.**
- **The County** will authorize appropriate employees and contractors to facilitate The Contractors deployment and provision of IT and cyber security services detailed in **Attachment A.**
- **The County** will provide a primary representative, employees and contractors as-needed during **The Contractors** installation and configuration of network security appliances (up to 2.5 days) as detailed in **Attachment A.**
- **The County** will provide feedback and status reports on an as-needed basis to **The State** to confirm **The Contractors** satisfactory installation and deployment of network security appliance and provision of IT and cyber security services detailed in **Attachment A.**
- In the event of an applicable IT or cybersecurity incident, **The County** will follow the ***"IT or cyber security incident notification protocol"*** provided by **The State**, which will include prompt notification of designated parties as soon as possible. or in no event later than 24 hours, of an applicable IT or cyber security incident.
- In the event of an applicable IT or cyber security incident, **The County** may apply to **The State** for ***Incident Responses Services*** which may be provided at the discretion of **The State**. Utilization of ***Incident Response Services*** by **The County** may obligate **The County** to incidental expenses as detailed in **Attachment B.**
- In the event of an applicable IT or cyber security incident, **The County** will use its best efforts to preserve forensic evidence and facilitate investigation and response by **The Contractors** and law enforcement agencies.
- **The County** will, throughout the term of **This Agreement** be responsible for its own efforts and incidental expenses associated with deployment and provision of IT and cyber security services and optional ***Incident Response Services.***
- At the end of the term of **The Contractors** provision services, **The County** will accommodate removal of provided security appliances and cessation of services.

P19/22

Attachment D

Responsibilities of The State

Tasks for which **The State** are responsible under **This Agreement** are:

- **The State** will coordinate contracting, administration and funding **The Contractor's** activities and provision of IT and cyber security services detailed in **Attachment A** and optional provision ***Incident Response Services*** if needed and approved, as detailed in **Attachment B**. The State is ***not*** obligated to incur or reimburse on behalf of **The County**, incidental ***Incident Response Services*** expenses detailed in **Attachment B**.

- **The State** will coordinate the business relationship between points of contact for **The County** and **The Contractors.**

- On an as-needed basis, **The State** will coordinate discussion and planning, kick-off meetings, network infrastructure analysis, configuration workshops, and status updates with, and between, representatives of the **The County** and **The Contractors.**

- **The State** will provide points of contact for **The County** and ***"IT or cyber security incident notification protocol"*** for notification of security incidents and technical issues pertaining to IT and cyber security services and optional ***Incident Response Services*** provided by **The Contractors.**

P20/22

Attachment E

FEDERAL REQUIREMENTS

Reference to "Contractor" shall mean the County. References to "this Contract" shall mean the Data Exchange Agreement.

1. **AUDITS AND ACCESS TO RECORDS:**

A. The Contractor acknowledges that some or all of the funds for this Contract are from a U.S. Department of Commerce ("DOC") grant. The Indiana Department of Technology, the U.S. Department of Commerce, the Comptroller General of the United States, or any of their duly authorized representatives shall have access to any books, documents, papers, and records that are pertinent to this Contract for the purpose of making an audit, examination, excerpts, and transcriptions. Unless a longer retention period is required by 44 CFR 13.42; these materials shall be maintained by the Contractor and made available at their respective offices at all reasonable times until January 27, 2018. Copies thereof shall be furnished at no cost. The rights of access in this provision are not limited to the required retention period but shall last as long as the records are retained.

B. The Contractor shall comply with the OMB Circulars A-87 (Cost Principles for State, Local and Tribal Governments) and 15 CFR 24 (UNIFORM ADMINISTRATIVE REQUIREMENTS FOR GRANTS AND COOPERATIVE AGREEMENTS TO STATE AND LOCAL GOVERNMENTS).

2. **INTELLECTUAL PROPERTY RIGHTS**

A. Data, Databases, and Software. The rights to any work produced or purchased under a DOC Federal financial assistance award are determined by 15 CFR § 24.34 and 15 CFR § 14.36. Such works may include data, databases or software. The recipient owns any work produced or purchased under a DOC Federal financial assistance award subject to DOC's right to obtain, reproduce, publish or otherwise use the work or authorize others to receive, reproduce, publish or otherwise use the data for Government purposes.

B. Copyright. The recipient may copyright any work produced under a DOC Federal financial assistance award subject to DOC's royalty-free nonexclusive and irrevocable right to reproduce, publish or otherwise use the work or authorize others to do so for Government purposes. Works jointly authored by DOC and recipient employees may be copyrighted but only the part authored by the recipient is protected because, under 17 U.S.C. § 105, works produced by Government employees are not copyrightable in the United States. On occasion, DOC may ask the recipient to transfer to DOC its copyright in a particular work when DOC is undertaking the primary dissemination of the work. Ownership of copyright by the Government through assignment is permitted by permitted by 17 U.S.C. § 105.

3. **DEBARMENT AND SUSPENSION.** As required by 2 CFR 3000.332, the Contractor shall:

A Comply with Subpart C of the OMB guidance in 2 CFR part 180; and

B Include a similar term or condition in any covered transaction into which it enters at the next lower tier.

4. **LOBBYING CERTIFICATION**

A. The Contractor acknowledges that a Federal grant is the source of payments under this Contract and as required by Section 1352, Title 31 of the U.S. Code, and implemented at 44 CFR Part 18, the Contractor certifies that:

(1) No Federal appropriated funds have been paid or will be paid, by or on behalf of the Contractor, to any person for influencing or attempting to influence an officer or employee of a federal agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any federal contract, the making of any Federal grant, the making of any federal loan, the entering of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

(2) If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any federal agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form - LLL, "Disclosure of Lobbying Activities," in accordance with its instructions;

P 21/22

(3) The Contractor shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, contracts under grants loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

B. This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by section 1352, title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

6. TRAFFICKING IN PERSONS

A. Provisions applicable to a recipient other than a private entity. The Federal Awarding Agency may unilaterally terminate this award, without penalty, if a subrecipient that is a private entity:

i. Is determined to have violated an applicable prohibition in paragraph A.i., above; or

ii. Has an employee who is determined by the agency official authorized to terminate the award to have violated an applicable prohibition in paragraph A.i, above, through conduct that is either:

a. Associated with performance under this award; or

b. Imputed to the subrecipient using the standards and due process for imputing the conduct of an individual to an organization that are provided in 2 CFR part 180, "OMB Guidelines to Agencies on Government-wide Debarment and Suspension (Non-procurement)," as implemented by the Federal Awarding Agency at 2 CFR part 3000.

B. Provisions applicable to any recipient.

i. You must inform the Federal Awarding Agency and the State immediately of any information you receive from any source alleging a violation of a prohibition in paragraph A.i, above.

ii. The Federal Awarding Agency's right to terminate unilaterally that is described in paragraph A.ii or B, above:

a. Implements section 106(g) of the Trafficking Victims Protection Act of 2000 (TVPA), as amended (22 U.S.C. 7104(g)), and

b. Is in addition to all other remedies for noncompliance that are available to the Federal Awarding Agency under this award.

iii. You must include the requirements of paragraph A.i,, above, in any subaward you make to a private entity.

C. Definitions. For purposes of this award term:

i. "Employee" means either:

a. An individual employed by you or a subrecipient who is engaged in the performance of the project or program under this award; or

b. Another person engaged in the performance of the project or program under this award and not compensated by you including, but not limited to, a volunteer or individual whose services are contributed by a third party as an in-kind contribution toward cost sharing or matching requirements.

ii. "Forced labor" means labor obtained by any of the following methods: the recruitment, harboring, transportation, provision, or obtaining of a person for labor or services, through the use of force, fraud, or coercion for the purpose of subjection to involuntary servitude, peonage, debt bondage, or slavery.

iii. "Private entity" means:

a. Any entity other than a State, local government, Indian tribe, or foreign public entity, as those terms are defined in 2 CFR 175.25.

P22/22