Item #10
03/16/21

INFORMATION TECHNOLOGY
400 West Fourth Street
Davenport, Iowa 52801-1104

Ph: (563) 328-4100 Fax: (563) 326-8669
www.scottcountyiowa.com

March 9, 2021

To: Mahesh Sharma, County Administrator

From: Matt Hirst, Information Technology Director

Subject: State of Iowa OCIO - Scott County Memorandum of Understanding

Attached is a Memorandum of Understanding between the State of Iowa Office of the Chief Information Officer (OCIO) and Scott County providing a framework for technology services between State of Iowa OCIO and Scott County. The agreement details technology services which could and are provided by the State of Iowa OCIO to Scott County.

I recommend that the Board approve this agreement as submitted.

Cc: Roxanna Moritz, Scott County Auditor

Encl: (1)

MEMORANDUM OF UNDERSTANDING ("MOU")

FOR

ENHANCED SECURITY SERVICES ("ESS")

BETWEEN

THE OFFICE OF THE CHIEF INFORMATION OFFICER OF THE STATE OF IOWA ("OFFICE")

AND

STATE AND LOCAL GOVERNMENTAL ENTITIES ("CUSTOMER")

This Memorandum of Understanding, including any attachments or exhibits hereto (**"MOU"**), for Enhanced Security Services, effective as of the date of last signature, below, is between the Office of the Chief Information Officer of the State of Iowa (**"Office"**) and the state or local governmental entity identified in the signature block below (**"Customer"**). In the event of a conflict or inconsistency between the terms and conditions set forth in the body of this MOU and any attachments or exhibits hereto, the terms and conditions in the body of this MOU shall take precedence. The parties may be referred to herein individually as a **"Party"** or collectively as the **"Parties."** The Parties agree to the following:

1. **Purpose.** The Office's mission is to "provide high-quality, customer-focused information technology services and business solutions to government and to citizens." Iowa Code § 8B.3(2). In this role, the Office provides Information Technology Services to governmental entities at both the State and local level. Iowa Code § 8B.12(1) (authorizing the Office to "enter into agreements with state agencies . . . and . . . any other governmental entity . . . to furnish services and facilities of the office to the applicable governmental entity"). Further, as Iowa's economy is becoming increasingly more reliant on technology, and in light of the increased frequency of significant cyber attacks, it is more important than ever to take action to secure computer networks and information systems. To aid governmental entities in guarding against significant cyber attacks that could adversely impact their ability to deliver mission critical services, threaten lifeline critical infrastructure, or otherwise negatively impact the public health, safety, welfare, or information security, the Office, through its Information Security Division (**"ISD"**), provides Enhanced Security Services (**"ESS"**) to governmental entities in the State of Iowa, including through its Security Operations Center (**"SOC"**). This MOU establishes the terms and conditions pursuant to which the Office provides these ESS, including through the SOC.

2. **Authority.** Pursuant to Iowa Code section 8B.12(1), "[t]he chief information officer shall enter into agreements with state agencies, and may enter into agreements with any other governmental entity .

. . , to furnish services and facilities of the office to the applicable governmental entity . . . . The agreement shall provide for the reimbursement to the office of the reasonable cost of the services and facilities furnished. All governmental entities of this state may enter into such agreements." In addition, pursuant to Iowa Code section 8B.21(1)(*i*), the Office is authorized to "[e]nter[] into . . . memorandums of understanding . . . or other agreements as necessary and appropriate to administer [Iowa Code chapter 8B]."

3. Duration. The term of this MOU shall be from the date of last signature below and shall continue unless and until terminated in accordance with the termination provision of this MOU (**"Term"**).

4. Definitions. Unless otherwise specifically defined in this MOU, all capitalized terms used herein shall have the meanings ascribed to them under Iowa Code chapter 8B and corresponding implementing rules found at Iowa Administrative Code chapter 129. In addition, the following terms shall have the following meanings:

4.1. **"Authorized Contractor(s)"** means independent contractors, consultants, or other Third Parties who are retained, hired, or utilized by the Office, in its sole discretion, to provide ESS, including through the SOC, or Office-Supplied Tools pursuant to and in accordance with the terms and conditions of this MOU.

4.2. **"Confidential Information"** means, subject to any applicable federal, State, or local laws and regulations, including Iowa Code Chapter 22, any information disclosed by either Party (**"Disclosing Party"**) to the other Party (**"Receiving Party"**) that, at the time of disclosure, is designated as confidential (or like designation), is disclosed in circumstances of confidence, or would be understood by the Parties, exercising reasonable business judgment, to be confidential. Confidential Information does not include any information that: (i) was rightfully in the possession of the Receiving Party from a source other than the Disclosing Party prior to the time of disclosure of the information by the Disclosing Party to the Receiving Party; (ii) was known to the Receiving Party prior to the disclosure of the information by the Disclosing Party; (iii) was disclosed to the Receiving Party without restriction by an independent Third Party having a legal right to disclose the information; (iv) is in the public domain or shall have become publicly available other than as a result of disclosure by the Receiving Party in violation of this MOU or in breach of any other agreement with the Disclosing Party; (v) is independently developed by the Receiving Party without any reliance on Confidential Information disclosed by the Disclosing Party; (vi) is disclosed in accordance with Section 9.3 (Compelled Disclosures) of this MOU; (vii) is disclosed as permitted by Section 8 (Information Exchanges, Third-Party Access, and Cloud Storage/Processing) of this MOU; or (viii) is disclosed by the Receiving Party with the written consent of the Disclosing Party. Subject to the foregoing exclusions, Confidential Information includes Customer Data.

4.3. **"Customer Data"** means all data or information originating with, disclosed by, provided by, made accessible by, or otherwise obtained by or from Customer in connection with this

MOU and the ESS provided hereunder, regardless of form. Generally, the Customer Data disclosed by, provided by, made accessible by, or otherwise obtained by or from Customer in connection with this Agreement and the ESS provided hereunder includes **"System Data"** such as security or software logs, system event information, system audit logs and records, and other similar information, as opposed to **"User Data"** such as files, database entries, or electronic records created by end users for governmental or business purposes.

4.4. **"Customer Systems"** means Customer's web sites, applications, databases, data centers, servers, networks, desktops, endpoints, or any other like systems or equipment (including as may be licensed or leased from, operated or managed by, or otherwise owned or originating with or from Third Parties) that are monitored, assessed, defended, or otherwise accessed by the Office in the performance of the ESS, including through the SOC, and which Customer Systems may be more fully identified and described in **Exhibit A**.

4.5. **"Enhanced Security Services"** or **"ESS"** or **"Services"** means the security services or any related services offered and provided by the Office, by and through the ISD, directly or indirectly, including through the SOC, which services are designed to assist governmental entities in the State of Iowa in:

4.5.1. Safeguarding against unauthorized access, disclosure, theft, or modification of or to government systems and data; and

4.5.2. Preventing, detecting, and responding to Security Incidents, Security Breaches, and other significant cyber events.

Enhanced Security Services include the services identified in **Exhibit A**.

4.6. **"Office-Supplied Tools"** means any hardware, equipment, software, applications, or tools (including software, applications, or tools running or installed on Third-Party networks, servers, operating systems, platforms, or infrastructure that are not managed or controlled by the Office (**"Third-Party Cloud Services"**)) installed by or on behalf of, or otherwise utilized by, the Office, directly or indirectly, on, or in a manner: designed to interface with or connect to, Customer Systems; that host, store, process, or transmit Customer Data; or that are otherwise used by the Office in connection with provisioning the ESS hereunder.

4.7. **"Security Breach"** means an occurrence that actually jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. **"Security Breach"** shall also be deemed to include any breach of security, confidentiality, or privacy as defined by any applicable law, rule, regulation, or order.

4.8. **"Security Incident"** means an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of

violation of security policies, security procedures, or acceptable use policies.

4.9. **"Security Operations Center"** or **"SOC"** means the State of Iowa's dedicated site and unit from and by which Customer Systems and Customer Data are monitored and assessed to detect Security Incidents, Security Breaches, and other significant cyber events that may result in unauthorized access, disclosure, theft, or modification of or to government systems or data.

4.10. **"Third Party"** means a person or entity (including, any form of business organization, such as a corporation, partnership, limited liability corporation, association, etc.) that is not a party to this MOU.

5. Office's Services. The Office, in exchange for the compensation paid by Customer in accordance with Section 10 (Compensation), will provide ESS, including through the SOC, to Customer in accordance with the terms and conditions of this MOU. In so doing, the Office will:

5.1. Work with Customer to identify and implement the ESS requested by Customer, as identified and agreed to in a fully executed **Exhibit A**.

5.2. Assess the severity of Security Incidents, Security Breaches, and other cyber events of which the Office is alerted to or otherwise becomes aware through the SOC; notify Customers of such events that may impact or involve Customer Systems or Customer Data; and work with Customers to remediate such events where possible.

5.3. Assist Customer in identifying Third Parties who are qualified to provide forensic investigative services that may be necessary to determine the full scope or impact of a Security Incident, Security Breach, or other cyber event that impacts or involves Customer Systems or Customer Data.

5.4. Provide any other ESS or related services as may be mutually agreed to by the Parties and as identified in **Exhibits A**.

6. Brokered I.T. Devices and Services. In addition to or in lieu of the Services or Office-Supplied Tools provided by the Office by more direct means hereunder, the Office may enter into Information Technology Master Agreements with Information Technology Vendors pursuant to which Customer may purchase Information Technology Devices or Services intended to enhance Customer's overall security posture and readiness. Where Customer purchases Information Technology Devices and Services pursuant to an Information Technology Master Agreement made available by the Office, such purchase shall constitute a separate, distinct, and independent contract between Customer and the applicable Vendor; Customer shall be solely responsible for any payments due and duties and obligations otherwise owed such Vendor under such agreement. In addition, OCIO bears no obligation or liability for Customer's losses, liabilities, or obligations, including Vendor's failure to perform, arising out of or relating in any way to such purchase. Likewise, the State of Iowa generally bears no obligation or liability for Customer's losses, liabilities, or obligations, including Vendor's failure to perform, arising out of or relating in any

way to such purchase.

7. **Customer's Responsibilities.** Customer is responsible for:

7.1. Obtaining and installing any hardware, equipment, software, applications, or tools, including Third-Party Cloud Services, to enable the Office to provide the ESS hereunder, including through the SOC. The Office will work to provide Customer with Office-Supplied Tools where possible, but where it is unable to do so or unable to obtain funding to do so, Customer may be responsible for doing so at Customer's own cost or expense, or have to forego the ESS provided hereunder, including through the SOC, or aspects thereof.

7.2. Granting and facilitating the Office access to any Customer Systems or facilities as is necessary for the Office to install or connect any Office-Supplied Tools as is necessary to enable the Office to provide the ESS hereunder, or directly installing or connecting such Office-Supplied Tools on or to Customer Systems as directed by the Office.

7.3. Working collaboratively with the Office, including providing appropriate staff to attend meetings and to address matters related to this MOU and the Office's provision of the ESS provided hereunder.

7.4. Protocols for Security Incident, Security Breach, and cyber event notification, handling, containment, and response are as may be set forth and described in **Exhibit A**, including:

7.4.1. Identifying Customer's point of contact who the Office should notify during normal business hours and off hours in the event the Office identifies a Security Incident, Security Breach, or other significant cyber event that may impact or involve Customer Systems or Customer Data;

7.4.2. Identifying under what circumstances, if any, the Office may act, unilaterally and without prior approval, to contain a Security Incident, Security Breach, or other significant cyber event that may impact or involve Customer Systems or Customer Data, or under what circumstances the Office must obtain prior approval from Customer prior to containing such event.

7.5. Determining whether a Security Incident, Security Breach, or other cyber event reported to Customer by the Office constitutes a security breach or other privacy or confidentiality violation or event for purposes of any reporting, notification, or other obligations that may be required by applicable law, rule, or regulation.

7.6. Reporting any Security Incident, Security Breach, or other cyber event to appropriate law enforcement or other relevant authority and notifying any consumers or other adversely affected individuals as may be required by applicable law, rule, or regulation.

7.7. Conducting forensic investigations that may be necessary to determine the full scope or impact of a Security Incident, Security Breach, or other cyber event. Generally, the ESS provided by the Office do not include forensic investigations, although the Office may assist

Customer in identifying Third Parties who are qualified to provide such services.

7.8. Not Misusing the Services or Office-Supplied Tools provided or performed by the Office, directly or indirectly, hereunder. Each of the following constitutes a **"Misuse(ing)"** for purposes of this MOU:

7.8.1. Using the Services or Office-Supplied Tools in a manner that is inconsistent with the Office's directions or instructions.

7.8.2. Using the Services or Office-Supplied Tools in a manner that is inconsistent with any applicable Third-Party license agreement or terms and conditions governing the use thereof.

7.8.3. Indirectly providing the Services or Office-Supplied Tools to unauthorized Third Parties, including through a service bureau or other like arrangement.

7.8.4. Using the Office's Services or Office-Supplied Tools in a manner that infringes, violates, or misappropriates any patent, trademark, copyright, trade dress, trade secret, or any other intellectual property right or proprietary right of the Office, the State, or any Third Party.

7.8.5. Using the Services or Office-Supplied Tools in a manner that is inconsistent with or violates applicable law, rule, or regulation.

7.8.6. Using the Services or Office-Supplied Tools in a manner that does not directly further the Customer's governmental objectives.

8. Information Exchanges, Third-Party Access, and Cloud Storage/Processing.

8.1. *Information Exchanges*. The SOC exchanges security incident information and analysis with a variety of Third Parties, including federal, state, and not-for-profit cybersecurity organizations such as, by way of example only, the United States Department of Homeland Security, Iowa Homeland Security & Emergency Management, the Iowa National Guard, Iowa Secretary of State, and Multi-State Information Sharing and Analysis Center (MS-ISAC). These information exchanges enable the Office to stay informed about evolving threats at national and regional levels, and to integrate such information into the Office's understanding and analysis of the state and local threats it monitors in real-time through the SOC. This results in improved analysis and security assessments overall. By entering into this MOU, Customer acknowledges, consents to, and authorizes the Office's exchange of such threat information with these Third Parties, including Security Incident, Security Breach, cyber event, and other threat information originally observed, obtained, or derived on or from Customer's Systems or Customer Data.

8.2. *Third-Party SOC Access*. The Office may grant access to the SOC to certain Third Parties to enable these Third Parties to monitor Customer Systems and Customer Data in furtherance of the Third Party's official duties. For example, in connection with an election, the Office

may grant the Iowa National Guard, operating in accordance with an active-duty order, access to the SOC to monitor Customer Systems that may be utilized or involved in facilitating election-related processes. As another example, the Office may grant the U.S. Department of Homeland Security access and connection to the SOC to conduct certain vulnerability assessments. Customer acknowledges, consents to, and authorizes the Office to grant these Third Parties access to the SOC, acknowledging that such access may permit these Third Parties to monitor Customer Systems and view or access Customer Data. In granting access to the SOC to any Third Party under this Section 8.2 (Third-Party SOC Access), the Office will limit the scope of such access to the data, tools, and systems, or relevant aspects thereof, comprising the SOC which permit the Third Party to accomplish its official duties, and implement reasonable and appropriate physical, technical, administrative, and organizational safeguards necessary to limit the scope of any such access. In addition, in granting access to the SOC to any Third Party under this Section 8.2 (Third-Party SOC Access), unless otherwise consented to and authorized by Customer following reasonable advance notice by the Office, the Customer Data that such Third Parties may be able to access or view through their access to the SOC will be limited to System Data as opposed to User Data.

8.3. *Cloud Storage/Processing*. Some of the Office-Supplied Tools utilized by the Office in providing the Services under this MOU include Third-Party Cloud Services. Customer acknowledges, consents to, and authorizes the Office to use Third-Party Cloud Services to supply the Services contemplated hereunder, acknowledging that such Third-Party Cloud Services may host, store, process, or transmit Customer Data.

9. Confidentiality.

9.1. *Office's Treatment of Customers Confidential Information*. The Office will implement and maintain reasonable and appropriate administrative, technical, and physical security measures to safeguard against unauthorized access, disclosure, theft, or modification of or to Confidential Information of, belonging to, or originating with Customer and will require the same of any Third Parties used in provisioning the Services or Office-Supplied Tools hereunder.

9.2. *Customer's Treatment of Office or Third-Party Confidential Information*. Confidential Information of, belonging to, or originating with the Office (such as training materials created, supplied, or provided by the Office or information and records concerning physical infrastructure, cyber security, critical infrastructure, security procedures, or emergency preparedness if disclosure could reasonably be expected to jeopardize life or property or other similar information, records, or related reports provided by the Office in performing the ESS created, supplied, or provided by the Office, including any records covered by Iowa Code section 22.7(50)) or Third Parties who supply or provide Office-Supplied Tools used by the Office in connection with the Services provided hereunder (including any Confidential Information embedded in or accessible through such Office-Supplied Tools),

shall at all times remain the property of the Office or applicable Third Party, and the Office or applicable Third Party shall retain exclusive rights thereto and ownership thereof. Customer may have access to such Confidential Information solely to the extent reasonably necessary to use the Services provided under this MOU. Customer shall hold such Confidential Information in confidence. Customer shall not gather, store, log, archive, use, or otherwise retain such Confidential Information in any manner other than as expressly authorized or contemplated by this MOU and will not disclose, distribute, sell, commercially or politically exploit, share, rent, assign, lease, or otherwise transfer or disseminate such Confidential Information to any Third Party, except as expressly permitted hereunder or as expressly approved by the Office in writing. Customer will immediately report the unauthorized access to or disclosure of such Confidential Information to the Office. Customer may be required to return and destroy, and provide proof of such return or destruction, such Confidential Information to the Office upon the expiration or termination of this MOU, as directed by the Office.

9.3. *Compelled Disclosures*. To the extent required by applicable law, rule, regulation, professional standards, subpoena, summons, or by lawful order or requirement of a court or governmental authority of competent jurisdiction over the Receiving Party, the Receiving Party may disclose Confidential Information to a Third Party in accordance with such law, rule, regulation, professional standards, subpoena, summons, lawful order, or requirement, subject to the following conditions:

9.3.1. As soon as becoming aware of such law, rule, regulation, professional standard, subpoena, summons, order, or requirement, and no-less-than five (5) business days prior to disclosing Confidential Information pursuant thereto, the Receiving Party will notify the Disclosing Party in writing, specifying the nature of and circumstances surrounding the contemplated disclosure, and forward any applicable source material, such as process or subpoena, to the Disclosing Party for its review.

9.3.2. The Receiving Party will consult with the Disclosing Party on the advisability of taking steps to resist or narrow any required response or disclosure.

9.3.3. The Receiving Party will use best efforts not to release Confidential Information pending the outcome of any measures taken by the Disclosing Party to contest, oppose, or otherwise seek to limit such disclosure by the Receiving Party and the Receiving Party will cooperate with the Disclosing Party regarding such efforts.

9.3.4. Solely the extent the Receiving Party is required to disclose Confidential Information to a Third Party, the Receiving Party will furnish only such portion or aspect of Confidential Information as it is required to disclose and will exercise reasonable efforts to obtain an order or other reliable assurances that any Confidential Information disclosed will be held in confidence by any Third Party

to which it is disclosed.

Notwithstanding any such compelled disclosure by the Receiving Party, such compelled disclosure will not otherwise affect the Receiving Party's obligations hereunder with respect to Confidential Information ultimately disclosed to a Third Party.

9.4. *Non-Exclusive Equitable Remedy*. Each Party acknowledges and agrees that due to the unique nature of Confidential Information, there can be no adequate remedy at law for any breach of its obligations hereunder, and therefore, that upon any such breach or any threat thereof, each Party will be entitled to appropriate equitable remedies, and may seek injunctive relief from a court of competent jurisdiction without the necessity of proving actual loss, in addition to whatever remedies either of might be available at law or equity. Any breach of this Section 9 (Confidentiality) will constitute a material breach of this MOU and will be grounds for the immediate termination of this MOU in the exclusive discretion of the non-breaching Party.

9.5. *Survives Termination.* Each Party's duties and obligations as set forth in this Section 9 (Confidentiality) shall survive termination of this MOU and shall apply to all acts or omissions taken or made in connection with the performance of this MOU regardless of the date any potential breach or claim is made or discovered by the other Party.

10. Compensation.

10.1. *SOC*. Customer agrees to pay the Office for the ESS provided through the SOC at the rates identified in **Exhibit A**.

10.2. *Hourly ESS/Consulting*. Certain ESS, such as consulting services, are available on a resource basis and are billed at hourly rates. Customer agrees to pay for such ESS consistent with the then-current service rates published at http://edas.iowa.gov. The Office reserves the right to alter these service rates from time to time. Customer is solely responsible for staying apprised of the Office's current service rates.

10.3. *Travel Costs*. Customer shall reimburse the Office for the actual cost of any transportation, meals, and lodging incurred by the Office in providing ESS to Customer pursuant to this MOU. Such Travel Costs shall not exceed the maximum reimbursement rates applicable to state personnel generally, including those set forth in the State Accounting Policy and Procedures Manual 210.245 and 210.305 or such other rates as may later be established by applicable laws, rules, policies or procedures.

10.4. *Pass-Through Costs and Expenditures*. Customer shall reimburse the Office for the actual cost of any Office-Supplied Tools or ESS provided by a Third-Party engaged directly by the Office for ESS or to provide ancillary services necessary to facilitate the Office's provision of ESS hereunder, such as installation services related to or involving Office-Supplied Tools. The Office may pass-through invoices it receives from these Third-Parties to Customer and Customer will reimburse the Office for the amount of such

Third Party services as set forth on the applicable invoice. This Section does not apply where Customer purchases directly from a Vendor or supplier pursuant to its own contract or an Information Technology Master Agreement made available by the Office in accordance with Section 6 (Brokered I.T. Devices and Services), in which case Customer shall be solely responsible for any payments due and duties and obligations otherwise owed such Vendor or supplier under such agreement.

10.5. *Invoices*. The Office shall invoice Customer on a monthly basis for fees due and owing from the prior month pursuant to this Section. Except where applicable law, rule, or ordinance requires otherwise, Customer shall pay all invoices within sixty (60) days and in arrears.

10.6. *Federal Funds.* Generally. Some of the ESS provided hereunder may be eligible to be paid for by funding awarded and available through the Homeland Security Grant Program (**"HSGP"**). The HSGP is administered by the Iowa Homeland Security and Emergency Management Division and is funded by U.S. Department of Homeland Security (DHS)/Federal Emergency Management Agency (FEMA). Whether and to what extent such funding is available shall be identified in **Exhibit A**. In the event such funding is available and used by the Office to pay for the ESS provided hereunder, Customer may not be required to pay the Office for ESS or other fees, costs, or expenses otherwise due and owing pursuant to this Section 10 (Compensation). If federal funding is available and its use is anticipated as identified in **Exhibit A**, the Office will provide reasonable notice to Customer should such funding availability or anticipated use change prior to continuing to provide such ESS under this MOU and permit Customer to determine whether it desires to leverage the ESS provided by the Office at the standard fees, costs, or expenses set forth in this Section 10 (Compensation).

11. DISCLAIMER OF WARRANTIES. THE OFFICE HEREBY DISCLAIMS ALL WARRANTIES, CONDITIONS, GUARANTEES AND REPRESENTATIONS RELATING TO THE ESS, OFFICE-SUPPLIED TOOLS, OR ANY ANCILLARY OR RELATED SERVICE PROVIDED OR MADE AVAILABLE BY THE OFFICE, DIRECTLY OR INDIRECTLY, IN CONNECTION IN WITH THIS MOU OR THE OFFICE'S, DIRECTLY OR INDIRECTLY, PERFORMANCE HEREOF, EXPRESS OR IMPLIED, ORAL OR IN WRITING, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND WHETHER OR NOT ARISING THROUGH A COURSE OF DEALING. THE ESS, INCLUDING THOSE PROVIDED THROUGH THE SOC, AND OFFICE-SUPPLIED TOOLS ARE NOT GUARANTEED TO BE ERROR-FREE OR UNINTERRUPTED.

12. Indemnification.

12.1. *Generally*. To the extent permitted by applicable law (including the Iowa Municipal Tort Claims Act (Iowa Code Chapter 670) and the Iowa Constitution), and without waiving any

of the immunities or protections available pursuant to applicable law, Customer agrees to indemnify and hold harmless the Office and State of Iowa, and their officers, employees, agents, appointed and elected officials, and volunteers (**"Indemnitee(s)"**) from and against any and all costs, expenses, losses, claims, damages, liabilities, settlements and judgments (including the reasonable value of the time spent by the Attorney General's Office, or the costs and expenses and reasonable attorneys' fees of any other counsel retained by the State of Iowa or the Office, in any litigation) related to or arising out of:

12.1.1. Any breach of this MOU by Customer or Customer's officers, employees, or agents;

12.1.2. Any negligent, intentional, wrongful, or unlawful act or omission of Customer or any employee or agent utilized or employed by Customer;

12.1.3. The Office's or any Indemnitee's infringement, violation, or misappropriation of any patent, trademark, copyright, trade dress, trade secret, or any other intellectual property right or proprietary right of any Third Party, but only to the extent such infringement, violation, or misappropriation is caused by, in whole or in part, the Office's access to or connection to Customer Systems, including as it relates to the installation or connection of or to any Office-Supplied Tools thereon or thereto;

12.1.4. Customer's infringement, violation, or misappropriation of any patent, trademark, copyright, trade dress, trade secret, or any other intellectual property right or proprietary right of any Third Party related to Customer's use of Office-Supplied Tools; or

12.1.5. Any Misuse of the Services or Office-Supplied Tools.

12.2. *First-Party Claims*. Customer's obligations under this Section 12 (Indemnification) are not limited to third-party claims but shall also apply to any claims the State of Iowa or Office may assert against Customer.

12.3. *Survival*. Customer's duties and obligations as set forth in this Section 12 (Indemnification) shall survive termination of this MOU and shall apply to all acts or omissions taken or made in connection with the performance of this MOU regardless of the date any potential breach or claim is made or discovered by the Office or State of Iowa.

12.4. *Applicability*. This Section 12 (Indemnification) shall be of no force and effect if Customer is or is part of an Iowa regent institution or State of Iowa agency.

13. Termination.

13.1. *Generally*. Following forty-five (45) days written notice, either Party may terminate this MOU, in whole or in part, for convenience without the payment of any penalty or incurring any further duty or obligation. Termination for convenience may be for any reason or no

reason at all. In the event of the expiration or termination of this MOU, Customer shall immediately cease using and return to the Office, as directed by the Office, Office-Supplied Tools or other Office- or State-owned or licensed property. Customer's duties and obligations set forth in this Section 13 (Termination) shall survive termination of this MOU.

13.2. *Notice Calculated to Enable Acquisition of Replacement Services*. While forty-five (45) days prior written notice is sufficient to terminate this MOU, in whole or in part, and cease providing any or all Services provided hereunder, the Office will, where possible, endeavor to provide additional and reasonable advance notice to Customer of the Office's intention to cease providing any or all Services hereunder, which advance notice shall be calculated to enable Customer to plan for the Office's discontinuation of applicable Services and to procure comparable replacement services. In determining what is reasonable under the circumstances, the Office will consider the likely impact of discontinuing any Services to Customer's operations, and the ability of and time it would take Customer to obtain comparable replacement services.

14. Administration.

14.1. *Relationship between the Parties*. The Office, its employees, agents and any subcontractors performing under this MOU are not employees or agents of Customer simply by virtue of work performed pursuant to this MOU. Neither the Office nor its employees shall be considered employees of Customer for federal or state tax purposes simply by virtue of work performed pursuant to this MOU. Likewise, this MOU shall not constitute or otherwise imply a delegation of either Party's legal duties or responsibilities to the other, or constitute, create, or imply a joint venture, partnership, or formal business organization of any kind. Neither Party shall be considered an agent, designee, or representative of the other for any purpose. No Party, unless otherwise specifically provided for herein, has the authority to enter into any contract or create an obligation or liability on behalf of, in the name of, or binding upon another Party to this MOU.

14.2. *Compliance with Law*. Both Parties and their employees, agents, and subcontractors shall comply with all applicable federal, state, and local laws, rules, regulations, orders, ordinances, and permitting requirements in the performance of their respective duties, responsibilities, and roles under this MOU.

14.3. *Choice of Law and Forum*. This MOU shall be governed in all respects by, and construed in accordance with, the laws of the State of Iowa, without giving effect to the choice of law principles thereof. In the event any proceeding of a quasi-judicial or judicial nature is commenced in connection with this MOU, any such proceeding shall be commenced in, and the exclusive jurisdiction for the proceeding shall be, Polk County District Court for the State of Iowa, Des Moines, Iowa, or in the United States District Court for the Southern District of Iowa, wherever jurisdiction is appropriate. This provision shall not be construed

as waiving any immunity to suit or liability, including sovereign immunity in State or Federal court, which may be available to the Office or the State of Iowa. Notwithstanding the foregoing or anything else in this MOU to the contrary, if Customer is a governmental agency of the State of Iowa, any dispute involving or stemming from this MOU shall not be brought in any of the aforementioned tribunals, but shall be submitted to binding arbitration pursuant to and in accordance with Iowa Code section 679A.19.

14.4. *Escalation of Disputes*. Should a disagreement involving or stemming from this MOU arise between the Parties that cannot be resolved, and prior proceeding to litigation or any other formal dispute resolution process in accordance with Section 14.3 (Choice of Law and Forum), the area(s) of disagreement shall be stated in writing by each Party and presented to the other Party for consideration. If an agreement is not reached within thirty (30) days, the Parties shall forward the written presentation of the disagreement to higher officials within their respective organizations for appropriate resolution. In the event the Parties are unable to reach an agreement after having completed that process, the parties may then, and only then, proceed to litigation or any other formal dispute resolution process in accordance with Section 14.3 (Choice of Law and Forum).

14.5. *Amendments*. This MOU may be amended in writing from time to time by mutual consent of the Parties. Any such amendments must be in writing and fully executed by the Parties.

14.6. *No Third-Party Beneficiary Rights*. There are no third party beneficiaries to this MOU. This MOU is intended only to benefit the Office and Customer.

14.7. *Assignment and Delegation*. This MOU may not be assigned, transferred, or conveyed, in whole or in part, without the prior written consent of the other Party.

14.8. *Entire Agreement.* This MOU represents the entire agreement between the Parties concerning the subject matter hereof. The Parties shall not rely on any representation, oral or otherwise, that may have been made or may be made and which is not included in this MOU. Each Party acknowledges that is has thoroughly read this MOU, and any amendments hereto as may be executed from time to time, and has had the opportunity to receive competent advice and counsel necessary for it to form a complete understanding of all rights and obligations herein and to accept the same freely and without coercion of any kind. Accordingly, this MOU shall not be construed or interpreted against either Party on the basis of draftsmanship or preparation thereof.

14.9. *Supersedes Former MOUs*. This MOU supersedes all prior MOUs or agreements between the Parties concerning the subject matter hereof.

14.10. *Headings or Captions and Terms*. The section and paragraph headings or captions used in this MOU are for identification purposes only and do not limit or construe the contents of the sections, paragraphs, or provisions herein. Unless the context of this MOU clearly requires otherwise, references to the plural include the singular, references to the singular include the plural, and the word "or" has the inclusive meaning represented by the phrase

"and/or." The words "include" and "including" shall be deemed to be followed by the phrase "without limitation" or "but not limited to." The words "thereof," "herein," "hereunder," and similar terms in this MOU refer to this MOU and any related attachment and exhibits hereto as a whole and not to any particular provision of this MOU or any related attachment or exhibit hereto.

14.11. *Notices*. Any and all legal notices, designations, consents, offers, acceptances or any other communication provided for herein shall be given in writing by registered or certified mail, return receipt requested, by receipted hand delivery, by Federal Express, courier or other similar and reliable carrier which shall be addressed to each Party to the contacts and at the addresses identified in **Exhibit A**. Each such notice shall be deemed to have been provided (1) At the time it is actually received; (2) Within one (1) day in the case of overnight hand delivery, courier, or services such as Federal Express with guaranteed next day delivery; or (3) Within five (5) days after it is deposited the U.S. Mail in the case of registered U.S. Mail. From time to time, the Parties may change the name and address of a Party designated to receive notice. Such change of the designated person shall be in writing to the other Party.

14.12. *Severability*. If any provision of this MOU is determined by a court of competent jurisdiction to be invalid or unenforceable, such determination shall not affect the validity or enforceability of any other part or provision of this MOU.

14.13. *Authorization*. Each Party to this MOU represents and warrants to the other Party that:

14.13.1. It has the right, power and authority to enter into and perform its obligations under this MOU.

14.13.2. It has taken all requisite action (corporate, statutory, or otherwise, including obtaining review and approval from any governing boards, commissions, councils, or other like bodies where required by applicable law, rule, regulation, order, or charter) to approve execution, delivery and performance of this MOU, and that this MOU constitutes a legal, valid and binding obligation upon itself in accordance with its terms.

14.14. *Successors in Interest*. All the terms, provisions, and conditions of this MOU shall be binding upon and inure to the benefit of the Parties hereto and their respective successors, assigns, and legal representatives.

14.15. *Waiver*. Except as specifically provided for in a waiver signed by duly authorized representatives of the applicable Party, failure by either Party at any time to require performance by the other Party or to claim a breach of any provision of this MOU shall not be construed as affecting any subsequent right to require performance or to claim a breach.

14.16. *Cumulative Rights*. The various rights, powers, options, elections and remedies of any Party provided in this MOU shall be construed as cumulative and not one of them is exclusive of the others or exclusive of any rights, remedies, or priorities allowed either Party by law, and

shall in no way affect or impair the right of any Party to pursue any other equitable or legal remedy to which any Party may be entitled.

14.17. *Exclusivity*. This MOU is not exclusive. Customer may obtain similar or identical Services, or cooperate or collaborate on other similar projects, from or with Third Parties.

14.18. *Multiple Counterparts and Electronic Signatures*. This MOU, including any amendments hereto, may be executed in several counterparts, all of which when taken together shall constitute one agreement binding on all Parties, notwithstanding that all Parties are not signatories to the same counterpart. Each such document(s) shall constitute an original. Signatures on such documents executed, scanned, and transmitted electronically and electronic signatures shall be deemed original signatures, with such scanned and electronic signatures having the same legal effect as original signatures. Such documents may be accepted, executed, or agreed to through the use of an electronic signature in accordance with the Electronic Signatures in Global and National Commerce Act (**"E-Sign Act"**), Title 15, United States Code, Sections 7001 et seq., the Uniform Electronic Transaction Act, codified at Iowa Code chapter 554D (**"UETA"**), or any other applicable state law, rule, policy, standard, directive, or order. Any document accepted, executed, or agreed to in conformity with such laws, rules, policies, standards, directives, or orders will be binding on the signing Party as if it were physically executed. Neither Party will contest the validity or enforceability of any such document(s), including under any applicable statute of frauds, because they were accepted, signed, or transmitted in electronic form. Each Party acknowledges and agrees that it will not contest the validity or enforceability of a signed scanned or facsimile copy of any such document(s) on the basis that it lacks an original handwritten signature, or on the basis that the Parties were not signatories to the same counterpart.

14.19. *Use of Trade Names*. Except as otherwise expressly permitted by this MOU, neither Party shall acquire any right to use, and shall not use, without the other Party's prior written consent, the other Party's trade names, trademarks, service marks, artwork, designs, copyrighted materials, or any other intellectual property.

14.20. *Use of Third Parties*. The Office may use Authorized Contractors to provide the Services or Office-Supplied Tools contemplated hereunder. Any rights, authorizations, or consents conferred or granted to the Office hereunder shall be deemed to be conferred or granted to and may be exercised by any Authorized Contractors used by the Office to provide the Services or Office-Supplied Tools contemplated hereunder.

14.21. *Force Majeure*. Neither Party shall be in default under this MOU if performance is prevented, delayed, or made impossible to the extent that such prevention, delay, or impossibility is caused by a "force majeure." The term "force majeure" as used in this MOU includes an event that no reasonable foresight could anticipate or which if anticipated, is incapable of being avoided. Circumstances must be abnormal and unforeseeable, so that the consequences could not have been avoided through the exercise of all due care, such as acts

of God, war, civil disturbance and other similar catastrophic events or causes. "Force majeure" for the Office includes: claims or court orders that restrict the Office's ability to perform or deliver the Services; strikes; labor unrest; supply chain disruptions; internet failures; power failures; hacker attacks; denial of service attacks; virus or other malicious software attacks or infections.

14.22. *Ancillary Agreements*. Generally, the Customer Data the Office, its Authorized Contractors, and other authorized Third Parties may be able to access or view in connection with this MOU will be limited to System Data as opposed to User Data. If access to or use of User Data is necessary to effectively provide the Services contemplated by this Agreement, the Office will provide Customer with notice prior to accessing or using any User Data in connection with the Services provided hereunder. The Office acknowledges that access to and use of User Data may require the execution of additional agreements to address unique compliance, legal, confidentiality, or privacy concerns, such as, where applicable, a Business Associate Agreement as may be required by the Health Insurance Portability and Accountability Act of 1996 (**"HIPAA"**), as amended. Upon mutual written agreement by the Parties, such **"Ancillary Agreements"** may be attached hereto as related special terms and conditions and incorporated by reference as if fully set forth herein. The Office may decline to execute such Ancillary Agreements and Customer acknowledges that, as a result, the Office may be unable to provide the contemplated Services, in whole or in part.

14.23. Review Meetings. The Office and Customer may meet on an annual basis to discuss the Services provided under this MOU, which may include discussion of any problems Customer has experienced in connection with the Services or areas for improvement or suggestions regarding new or additional service offerings. Customer authorizes the Iowa Counties Information Technology ("ICIT") organization, an affiliate of the Iowa State Association of Counties ("ISAC"), to represent its interests and perspective at these annual review meetings, and shall communicate any concerns or suggestions to ICIT, which will consolidate such concerns or suggestions and communicate them to the Office as part of these annual review meetings.

15. Customer Systems/Data Access and Liability.

15.1. Customer consents to and authorizes the Office to access and monitor Customer Systems and Customer Data to the extent necessary to perform the ESS contemplated hereunder. Such access and monitoring may be subject to mutually agreed upon protocols outlining appropriate information, network, and device connections, as may be further defined and described in **Exhibit A**. Such access and monitoring may include the following:

15.1.1. Administrator level and/or system-level access to any network, computing, or communications device;

15.1.2. Access for interactively monitoring and logging traffic on Customer Systems,

including Customer's networks; and

15.1.3. Access to information Customer Data that may be produced, transmitted, or stored on, from, or over Customer Systems, equipment, facilities, or premises.

15.2. Customer acknowledges that the ESS, including the ESS provided through the SOC, and installation or connection of Office-Supplied Tools to Customer Systems, or Customer's or the Office's use of Office-Supplied Tools that are Third-Party Cloud Services, involves a risk of potential adverse impacts or consequences to Customer Systems and Customer Data, including degradation, loss, or disruption of network and system performance or availability, or loss or destruction of Customer Data. Customer agrees to assume all risk for any damages, losses, expenses, and other adverse consequences resulting from or associated with the performance or provisioning of the ESS hereunder, including the ESS provided through the SOC, or that may otherwise result from the installation or connection of Office-Supplied Tools on Customer Systems or Customer's or the Office's use of Office-Supplied Tools that are Third-Party Cloud Services. Consistent with the foregoing, Customer waives any claims it may have against the Office or the State of Iowa involving Customer Property or Customer Data caused, in whole or in part, by the Office's provisioning of the ESS hereunder, including the ESS provided through the SOC, or installation or connection of Office-Supplied Tools to Customer Systems or Customer's or the Office's use of Office-Supplied Tools that are Third-Party Cloud Services.

15.3. The Office's provisioning of ESS hereunder, including through the SOC, including the Office's access to and monitoring of Customer Systems, may enable the Office to access and monitor Customer Systems and Customer Data, which may be owned and managed by Customer. Customer, in turn, may be or may be comprised of governmental entities, such as the State of Iowa, cities, or counties, or departments, boards, agencies, commissions, or councils comprising the foregoing. Customer represents and warrants that it has the authority to grant the Office the right to access and monitor such Customer Systems and Customer Data as contemplated in this MOU and has taken all requisite action (corporate, statutory, or otherwise, including obtaining review and approval from any governing boards, commissions, councils, or other like bodies where required by applicable law, rule, regulation, order, or charter) necessary to grant or permit access to and monitoring of the Customer Systems and Customer Data as contemplated by this MOU.

IN WITNESS WHEREOF, in consideration of the mutual covenants set forth above and for other good and valuable consideration, the receipt, adequacy and legal sufficiency of which are hereby acknowledged, the Parties have entered into MOU and have caused their duly authorized representatives to execute this MOU, which MOU takes effect on the date of last signature below.

Signature:_____ **Signature:**_____

Name (Printed):_____	**Name (Printed):**_____
Title: Chief Information Officer, State of Iowa	**Title:** _____
Organization signed on behalf of ("Office"): Office of the Chief Information Officer, State of Iowa	**Organization signed on behalf of ("Customer"):** _____
Date:_____	**Date:** _____

Exhibit A

Fee Schedule, Services Description, Access and Monitoring Protocols, and Security Incident/Breach Control/Reporting Protocols

This Exhibit A is part of and incorporated into the related Memorandum of Understanding (**"MOU"**) for Enhanced Security Services between the Office of the Chief Information Officer of the State of Iowa (**"Office"**) and the state or local governmental entity identified in the signature block below (**"Customer"**). Capitalized terms used but not defined herein are as defined in the MOU. In the event of a conflict or inconsistency between the terms and conditions set forth in this Exhibit A and the body of the MOU, the terms and conditions in the body of the MOU shall take precedence. The parties may be referred to herein individually as a **"Party"** or collectively as the **"Parties**."

1. Compensation.

1.1. *SOC Fees*. Presently, there are no fees for the SOC under the MOU. Customer's use of the ESS provided through the SOC are paid for by funding awarded and available through the HSGP grant. If any ESS provided beyond the scope of the SOC is agreed to by the Parties, such Services may not be covered by the HSGP grant, and the Office may require the Customer to execute an amended Exhibit A setting forth the fees for that particular Service.

1.2. *Federal Funds*. As contemplated by Section 10.6 (Federal Funds) of the MOU, the following ESS or Office-Supplied Tools are paid for by funding awarded and through the HSGP grant:

1.2.1. SOC. There are no fees for the SOC under the MOU. Customer's use of the ESS provided through the SOC are paid for by funding awarded and available through the HSGP grant.

1.2.2. Office-Supplied Tools. The following Office-Supplied Tools are paid for by funding awarded and available through the HSGP grant:

1.2.2.1. Intrusion Detection System (IDS);

1.2.2.2. Enterprise Vulnerability Management System (EVMS);

1.2.2.3. Anti-Malware (Host based and Network based);

1.2.2.4. Security Awareness Training and Phishing Tests;

1.2.2.5. Web Filtering.

1.2.2.6. Or any other ESS mutually agreed upon by the Parties the Office agrees to provide Customer, including by or through the SOC.

2. Customer Systems. For purposes of the MOU, including as it relates to the applicability of Section 15 of the MOU (Customer Systems/Data Access and Liability), Customer Systems include:

2.1. Customer's network equipment;

2.2. Customer's endpoints;

2.3. Any other of Customer's web sites, applications, databases, data centers, servers, networks, desktops, endpoints, or any other like systems or equipment (including as may be licensed or leased from, operated or managed by, or otherwise owned or originating with or from Third Parties) that are monitored, assessed, defended, or otherwise accessed by the Office in the performance of the ESS, or on which the Office has installed Office Supplied Tools or that otherwise interface with Office Supplied Tools in connection with the ESS provided hereunder.

3. Access, Monitoring and Response Protocols. The Office's access, monitoring and response is subject to the following mutually agreed upon protocols:

3.1. Access - SOC intends to limit access to Customer Data and Customer Systems to the extent necessary to identify a Security Incident or Security Breach or as needed for the appropriate configuration of Office Tools used in the provisioning of Services under the MOU. Generally, this means that if an alert requires a deeper investigation, prior to accessing or acquiring any additional User Data the Office will request customer permission to access such information from the alerting Customer System;

3.2. Monitoring - Customer Data and Customer Systems are only to be monitored for malicious activity, suspicious activity, risk identification, and vulnerabilities. Office-Supplied Tools relating to endpoint monitoring and protection Services will be installed by the Customer using installation files and instructions provided by the Office. The Office will work with Customer to identify areas where additional deployment opportunities exist to ensure maximum coverage for the Customer. Network monitoring and scanning devices are to be placed inside the Customer's network architecture where the highest network coverage and visibility can be attained. Customer will provide credentials as needed to obtain the most efficient monitoring and scanning configuration;

3.3. Response -

3.3.1. Specific response protocols will follow internal SOC reporting and notification procedures, which may be updated from time to time and provided to the Customer upon request.

3.3.2. The Office may act, unilaterally and without prior approval, to contain a Security Incident, Security Breach, or other significant cyber event where a cyber event is likely to have an adverse impact or cause damage to Customer Systems or Customer Data, including degradation, loss, or disruption of network and system performance or availability, or loss or destruction of Customer Data.

3.3.3. Notwithstanding the foregoing, the Office will not act unilaterally to contain a

cyber event for any specific Customer System or Customer device identified by Customer, in writing, and provided to the Office. By way of example only, several Customers have requested that the Office not act unilaterally to contain events related to 911 systems.

3.3.4. In containing a cyber event as permitted hereunder, the Office or its Authorized Contractors may briefly have access, actual or theoretical, to User Data. Customer acknowledges and consents to the Office's limited access to User Data consistent with the parameters of this Section 3.3, and the Office or its Authorized Contractors will not be required to execute Ancillary Agreements to contain a cyber event as permitted by this Section 3.3, provided access to User Data shall be limited to that purpose.

4. **Notices**. The point of contact for issues of or concerning the administration of this MOU, and individual and contact information to which notices under Section 14.11 (Notices) of the MOU should be addressed and sent, is the following:

For the Office:

Dan Powers
Manager, Information Security Division/Networking
200 E Grand
Des Moines, Iowa 50319
Phone: (515) 240-8226
Email: dan.powers@iowa.gov

For Customer:

Phone:
Email:

IN WITNESS WHEREOF, in consideration of the mutual covenants set forth above and for other good and valuable consideration, the receipt, adequacy and legal sufficiency of which are hereby acknowledged, the Parties have entered into Exhibit A and have caused their duly authorized representatives to execute this Exhibit A, which Exhibit A takes effect on the date of last signature below.

Signature:_____	**Signature:**_____
Name (Printed):_____	**Name (Printed):**_____
Title: Chief Information Officer, State of Iowa	**Title:** _____
Organization signed on behalf of ("Office"): Office of the Chief Information Officer, State of Iowa	**Organization signed on behalf of ("Customer"):** _____
Date:_____	**Date:** _____

THE COUNTY AUDITOR'S SIGNATURE CERTIFIES THAT THIS RESOLUTION HAS BEEN FORMALLY APPROVED BY THE BOARD OF SUPERVISORS ON

_____.
DATE

SCOTT COUNTY AUDITOR

R E S O L U T I O N

SCOTT COUNTY BOARD OF SUPERVISORS

March 18, 2021

A RESOLUTION APPROVING A MEMORANDUM OF UNDERSTANDING BETWEEN THE STATE OF IOWA OCIO AND SCOTT COUNTY

BE IT RESOLVED BY the Scott County Board of Supervisors as follows:

Section 1. The Memorandum of Understanding between the State of Iowa Office of the Chief Information Officer and Scott County defining technology services is hereby approved.

Section 2. This resolution shall take effect immediately.