**RESOLUTION APPROVING AN AGREEMENT WITH ELECTION SYSTEMS & SOFTWARE, LLC (ES&S) FOR HARDWARE MAINTENANCE AND SOFTWARE LICENSE, MAINTENANCE AND SUPPORT SERVICES AGREEMENT**

WHEREAS, the Board of Elections has presented an agreement for the approval of the Board, to-wit:

**Scope**: Election Systems & Software, LLC (ES&S) will provide hardware maintenance and software license, maintenance and support services for the voter tabulation equipment located at the Board of Elections.

**Provider:** Election Systems & Software, LLC, 11208 John Galt Blvd., Omaha, NE 68137

**Cost:** **Not to Exceed $332,340.00**

**Term:** retroactive to March 1, 2024 until February 28, 2029

THEREFORE, BE IT RESOLVED, By the Board of Commissioners of Ashtabula County, Ohio that the Agreement noted above is approved in accordance with the copy now on file in this office.

BE IT FURTHER RESOLVED that the President of the Board, on behalf of the Board of Commissioners of Ashtabula County, is authorized to execute any and all necessary documents.

**ASHTABULA COUNTY COMMISSIONERS**

**CERTIFICATION PAGE**

**Resolution No. 2024-406** **August 27, 2024**

**RESOLUTION APPROVING AN AGREEMENT WITH ELECTION SYSTEMS & SOFTWARE, LLC (ES&S) FOR HARDWARE MAINTENANCE AND SOFTWARE LICENSE, MAINTENANCE AND SUPPORT SERVICES AGREEMENT**

**Upon the motion of J.P. Ducro IV, seconded by Casey R. Kozlowski.**

**VOTE:**

| | |
|---|---|
| **Kathryn L. Whittington** | **Aye** |
| **J.P. Ducro IV** | **Aye** |
| **Casey R. Kozlowski** | **Aye** |

**CERTIFICATE OF CLERK**

IT IS HEREBY CERTIFIED that the foregoing is a true and correct transcript of a resolution acted upon and duly passed by the Board of County Commissioners of Ashtabula County, Ohio, on the date noted above.

Lisa Hawkins

Lisa Hawkins, Clerk of the Board
Board of County Commissioners
Ashtabula County, Ohio

**ELECTION SYSTEMS & SOFTWARE, LLC**
**HARDWARE MAINTENANCE AND SOFTWARE LICENSE, MAINTENANCE AND SUPPORT SERVICES AGREEMENT**

THIS HARDWARE MAINTENANCE AND SOFTWARE LICENSE, MAINTENANCE AND SUPPORT SERVICES AGREEMENT ("Agreement") is made effective as of the date set forth below, by and between Election Systems & Software, LLC, a Delaware Limited Liability Company ("ES&S") and **Ashtabula County, Ohio** ("Customer").

RECITALS:

A. ES&S has sold to Customer the proprietary voter tabulation equipment ("Equipment") and licensed the software ("Software") described on Attachment 1 and Customer now desires to obtain maintenance services for such Equipment and license, maintenance, and support services for such Software.

B. ES&S has agreed to provide such services, subject to the terms and conditions of this Agreement.

C. This Agreement supersedes and replaces in their entirely any and all prior agreements between ES&S and Customer respecting maintenance services for such Equipment and license, maintenance and support services for such Software.

NOW, THEREFORE, in consideration of the foregoing recitals (which are specifically incorporated herein by this reference) and the mutual representations, warranties, covenants and agreements set forth below, the parties hereby agree as follows:

## ARTICLE I
## GENERAL

1. **Term; Termination.** This Agreement for Hardware Maintenance and Software License, Maintenance and Support Services shall be in effect for the coverage period as described in Attachment 1 (the "Term"). This Agreement may be terminated by the first to occur of (a) the date which is thirty (30) days after either party notifies the other that it has materially breached this Agreement, if the breaching party fails to cure such breach (except for a breach pursuant to subsection (d), which will require no notice), (b) the date which is thirty (30) days after ES&S notifies Customer that it is no longer able to procure replacement parts that may be needed in order to perform the Hardware Maintenance Services contemplated hereunder, (c) the date on which the Equipment or firmware installed thereon is no longer certified by federal and/or state authorities for use in Customer's jurisdiction, (d) the date which is thirty (30) days after Customer fails to pay any amount due to ES&S under this Agreement, or (e) the date which is thirty (30) days after Customer provides written notice to ES&S that it desires to terminate this Agreement at any time during the Term. The termination of this Agreement shall not relieve Customer of its liability to pay any amounts due to ES&S hereunder and shall only entitle Customer to a prorated refund of any fees already paid to ES&S in the event this Agreement is terminated pursuant to subsection 1(a) or 1(b) above. In no event shall Customer be entitled to a refund of any fees paid in the event this Agreement is terminated pursuant to subsections 1(c), 1(d) or 1(e) above.

2. **Fees.** In consideration for ES&S' agreement to provide Hardware Maintenance Services and Software License, Maintenance and Support Services under this Agreement, Customer shall pay to ES&S the Hardware Maintenance and Software License, Maintenance and Support Fees set forth on Attachment 1 for the Term. The Hardware Maintenance and Software License, Maintenance and Support Fees for the Term are due as set forth on Attachment 1. The Software License, Maintenance and Support Fee shall be comprised of (i) a fee for the Software License, Maintenance and Support provided for the ES&S Firmware, and (ii) a fee for the Software License, Maintenance and Support provided for all other ES&S Software and shall be in addition to any fees or charges separately referred to in any Section of this Agreement. If Customer elects to receive Software License, Maintenance and Support for an Add-On or New Product during the Term, ES&S will charge an incremental Software License, Maintenance and Support Fee for such services.

## ARTICLE II
## HARDWARE

1. **Maintenance Services.** The Hardware Maintenance Services to be provided to Customer under this Agreement for the ES&S equipment set forth on Attachment 1 (the "Products") shall be subject to the following terms and conditions:

a. **Routine Maintenance Services.** An ES&S Representative shall provide such services as may be necessary to keep the Products working in accordance with their Documentation, normal wear and tear excepted ("Normal Working Condition"). The services provided by ES&S pursuant to this Subsection 1(a) are referred to herein as "'Routine Maintenance Services". Routine Maintenance Services shall be provided once each **Twenty-Four (24) Months** during the Term. Generally, Routine Maintenance Services shall include cleaning, lubrication, diagnostic check, and calibration services. The Routine Maintenance Services shall not include the repair or replacement of any ES&S Equipment components that are consumed in the normal course of operating the Equipment, including, but not limited to, headphones and headphone protective covers, printer cartridges or ribbons, paper, batteries, drums, toners, fusers, transfer belts, removable media storage devices, seals, keys, power supplies/cords, PCMCIA, Smart, or CF cards or marking devices (collectively, the "Consumables"). ES&S may modify and make available additional Consumables as they may become available from time to time. Customer may request that Routine Maintenance Services be performed more than once during the Term. Any such request shall be made at least sixty (60) days before the Routine Maintenance Services are desired. The per-unit fee for such additional Routine Maintenance Services is set forth on Attachment 1 and shall be due within thirty (30) days after invoice date. ES&S will schedule the Routine Maintenance Services with Customer. The Routine Maintenance Services will be provided at Customer's Designated Location. Customer's "Designated Location" shall mean Customer's owned or leased facility at which Customer desires ES&S to perform the Hardware Maintenance Services.

b. **Repair Services.**

i. **Defects Under Normal Use and Service.** If a defect or malfunction occurs in any Product while it is under normal use and service, Customer shall promptly notify ES&S, and ES&S shall use reasonable efforts to restore the item to Normal Working Condition as soon as practicable. The services provided by ES&S pursuant to this Subsection 1(b)(i) are referred to herein as "Repair Services". ES&S will perform Repair Services in conjunction with a Routine Maintenance Service event at the Customer's Designated Location.

ii. **Defects Due to Customer Actions or Omissions.** If a defect or malfunction occurs in any Product as a result of (1) repairs, changes, modifications or alterations not authorized or approved by ES&S, (2) use, modification, dismantling, disassembly, or transfer to third party without ES&S' prior written consent, (3) accident, theft, vandalism, neglect, abuse, liquid contact, use of adhesive materials on ballots or use that is not in accordance with instructions or specifications furnished by ES&S or (4) causes beyond the reasonable control of ES&S or Customer, including acts of God, fire, flooding, riots, acts of war, terrorism or insurrection, government acts or orders; epidemics, pandemics or outbreak of communicable disease; quarantines; national or regional emergencies, labor disputes, transportation delays, governmental regulations, and utility or communication interruptions, rodent infestation, or if Customer does not notify ES&S within 72 hours after it knows of the defect or malfunction, Customer shall pay ES&S for the Repair Services at ES&S' then-current rates, as well as for the cost of all parts used in connection with such Repair Services.

iii. **Timing.** The date(s) on which any Repair Services shall be provided shall be mutually agreed upon by ES&S and Customer. If Customer requires ES&S to provide "emergency" Repair Services (which shall be defined as Repair Services that are provided by ES&S within 48 hours after Customer notifies ES&S of the need therefore), and such emergency Repair Services are not needed as a result of an action, error or omission by ES&S, Customer shall pay a surcharge, as set forth on Attachment 1.

iv. **Loaner Unit.** At Customer's request and if such product is available, ES&S shall use reasonable efforts to promptly make available to Customer a product that is the same as, or substantially similar to, the Product for which Repair Services are being performed (a "Loaner Unit"). If the Repair Services are being performed pursuant to Subsection 1(b)(ii) above, Customer shall pay ES&S for the use of the Loaner Unit at ES&S' then-current rates including the cost of shipping.

c. **Exclusions.** ES&S has no obligation under this Agreement to (i) assume the obligations under any existing or expired warranty for a Third Party Item; (ii) repair or replace Product components that are consumed in the normal course of operating the Product, including, but not limited to, headphones and headphone protective covers, printer cartridges or ribbons, paper, batteries, drums, toners, fusers, transfer belts, removable media storage devices, seals, keys, power supplies/cords, PCMCIA, Smart, or CF cards or marking devices (collectively, the "Consumables"), or (iii) repair any Product from which the serial number has been removed or altered. In addition, ES&S may, at any time in its discretion, determine that any Product is no longer fit for Hardware Maintenance Services because it is in such poor condition that it cannot practically be restored to Normal Working Condition, or cannot be restored to Normal Working Condition at an expense that is less than the then-current value of the Product. If such a determination is made, ES&S shall no longer be required to provide Hardware Maintenance Services for such Product. ES&S shall also refund to Customer an amount equal to (1) that portion of the most recent fee paid for Hardware Maintenance Services that is attributable to such Product, multiplied by (2) a fraction, the numerator of which is the remaining number of days within the Term for which such fee was paid and the denominator of which is the total number of days within the Term.

d. **Sole Provider; Access.** Customer shall not permit any individual other than an ES&S Representative to provide maintenance or repairs with respect to the Products for so long as the Term is in effect. Customer shall provide ES&S Representatives with all information necessary to enable them to provide Hardware Maintenance Services. Customer shall likewise provide full access to the Products and adequate working space for all Hardware Maintenance Services performed at its Designated Location, including sufficient heat, lights, ventilation, electric current and outlets.

e. **Environment Conditions.** Products should be stored in a clean, dry, and secure environment. During the storage and operation of the Products, the temperature and moisture ranges should be maintained in accordance with the Product's Documentation.

f. **Reinstatement of Hardware Maintenance Services; Inspection.** If the Term expires, Customer may thereafter resume receiving Hardware Maintenance Services upon (a) notification to ES&S and (b) the granting to ES&S of access to the Products. ES&S requires Customer to allow it to inspect such Products before it provides any Hardware Maintenance Services. The purpose of such inspection shall be to determine whether or not the Products are in Normal Working Condition. The cost of such inspection will be at ES&S' then current rates and shall be due from Customer within thirty (30) days of its receipt of ES&S' invoice, therefore. If any of the Products is not in Normal Working Condition, ES&S, at the option of Customer, (i) shall provide such repairs and replacements as it deems reasonable and necessary to restore such item to Normal Working Condition, at Customer's expense with respect to the cost of any labor (charged at ES&S' then current rates) and parts used in such repairs or replacements, or (ii) shall not provide any Hardware Maintenance Services with respect to such Product(s).

## ARTICLE III
## ANNUAL LICENSE OF SOFTWARE

1. **Grant of License.** Subject to the terms and conditions of this Agreement, ES&S hereby grants to Customer a nonexclusive, nontransferable license for its bona fide full time, part time or temporary employees to use the Software and all related operating instructions, user manuals and training materials supplied by ES&S (collectively the "Documentation") in **Ashtabula County, Ohio** ("Jurisdiction"). The license allows Customer to use and copy the Software (in object code only) and the Documentation, solely for the purposes of defining an election and tabulating and reporting election results in the Jurisdiction. The license does not permit Customer to take any of the following actions:

a. Reverse engineer, decompile, disassemble, re-engineer or otherwise create, attempt to create, or permit, allow or assist others to create, the source code or the structural framework for part or all of the Software;

b. Cause or permit any use, display, loan, publication, transfer of possession, sublicensing or other dissemination of the Software or Documentation, in whole or in part, to or by any third party including, but not limited to, any transfer of possession to, or use of the ES&S Software or Documentation by any third party to perform any services for Customer (including, but not limited to, any coding, programming or layout services) without ES&S' prior written consent; or

c. Cause or permit any change to be made to the Software without ES&S' prior written consent.

d. Allow a third party to cause or permit any copying, reproduction or printing of any output generated by the Software (except finished ballots by ballot printers selected by Customer) in which ES&S owns or claims any proprietary intellectual property rights (e.g., copyright, trademark, patent pending or patent), including, but not limited to, any ballot shells or ballot code stock.

2. **License Fees**. In consideration for ES&S' grant of the license for the ES&S Software described in Section 1, Customer shall pay ES&S the ES&S Software License Fees set forth on Attachment 1. Any license or royalty fees payable to any Third Parties for the use of any third-party items are the sole responsibility of Customer.

3. **Term of License.** The Software License shall be in effect for the coverage period as described in Attachment 1 (the "License Term). ES&S may terminate the license if Customer fails to pay the consideration due for, or breaches Sections 1, 2, or 4 with respect to, such license. Upon the termination of the license granted in Section 1 for ES&S Software or upon Customer's discontinuance of the use of any ES&S Software, Customer shall immediately return such ES&S Software and the related Documentation (including any and all copies thereof) to ES&S, or (if requested by ES&S) destroy such ES&S Software and Documentation and certify in writing to ES&S that such destruction has occurred.

4. **Proprietary Rights.** Customer acknowledges and agrees that ES&S owns all right, title, and interest in and to the Software and Documentation, subject to the license granted herein. ES&S likewise owns all patents, trademarks, copyrights, trade names and other proprietary or intellectual property in, or used in connection with, the Software and Documentation. The Software and Documentation also contain confidential and proprietary trade secrets of ES&S which are protected by law and are of substantial value to ES&S. Customer shall keep the Software and Documentation free and clear of all claims, liens and encumbrances and shall maintain all copyright, trademark, patent or other intellectual or proprietary rights notices which are set forth on the Software, the Documentation, and all permitted copies thereof.

## ARTICLE IV
## SOFTWARE LICENSE, MAINTENANCE AND SUPPORT SERVICES

1. **Services Provided.** ES&S shall provide maintenance and support services ("Software License, Maintenance and Support") for the ES&S Software and ES&S Firmware (collectively, "ES&S Software"), to enable it to perform in accordance with its Documentation in all material respects, and to cure any defect in material or workmanship. The specific Software Maintenance and Support Services provided by ES&S and each party's obligations with respect to such services are set forth on Attachment 1.

2. **Updates.** During the License Term for which Customer has paid the associated fees, ES&S may provide new releases, upgrades, or maintenance patches to the ES&S Software, together with appropriate Documentation ("Updates"), on a schedule defined by ES&S. Customer is solely responsible for obtaining and purchasing any upgrades or Third-Party Items required to operate the Updates, as well as the cost of any replacements, retrofits or modifications to the ES&S Equipment which may be necessary in order to operate the Updates. All Updates shall be deemed to be ES&S Software for purposes of this Agreement upon delivery. Updates to the ES&S Equipment Firmware will be incorporated by ES&S into a regularly scheduled preventative maintenance event at no additional charge to Customer. If this foregoing is not acceptable to Customer and subject to Customer's prior execution of a purchase order therefore, ES&S shall charge to install the Updates to the ES&S

Equipment Firmware. ES&S shall also charge Customer at its then-current rates to; (i) train Customer on Updates, if such training is requested by Customer and (ii) if applicable, provide maintenance and support on the ES&S Software that is required as a result of Customer's failure to timely or properly install an Update. Notwithstanding the foregoing, Customer shall pay ES&S to install all election management software Updates. If applicable, Customer shall be responsible for any claim, damage, loss, judgment, penalty, cost, amount paid in settlement or fee which is caused by Customer's failure to install the most recent Update provided to it by ES&S. If Customer proposes changes in the ES&S Software to ES&S, such proposals will become ES&S' property. ES&S may, in its sole discretion, elect to make or not to make such changes without reference or compensation to Customer or any third party. ES&S represents to Customer that the Updates will comply with all applicable state law requirements at the time of delivery. Customer shall be responsible to ensure that it has installed and is using only certified versions of ES&S Software in accordance with applicable law. In the event that any Updates are required due to changes in state law, ES&S reserves the right to charge Customer for the following

(i) the total cost of any third-party items that are required in order to operate the Updates;

(ii) the total cost of any replacements, retrofits or modifications to the ES&S Equipment contracted for herein that may be developed and offered by ES&S in order for such ES&S Equipment to remain compliant with applicable laws and regulations; and

(iii) Customer's pro-rata share of the costs of designing, developing and/or certification by applicable federal and state authorities of such state mandated Updates.

Customer's pro-rata share of the costs included under subsection (iii) above shall be determined at the time by dividing the number of registered voters in Customer's jurisdiction by the total number of registered voters in all counties in Customer's state to which ES&S has sold and/or licensed the Equipment and/or Licensed Software purchased and licensed by Customer under this Agreement. Customer shall pay ES&S the entire costs incurred for design, development and certification of any Update which is required due to a change in local law or is otherwise requested or required by Customer.

3. **Conditions.** ES&S shall not provide Software License, Maintenance and Support for any item of ES&S Software if such item requires such services as a result of (a) repairs, changes, modifications or alterations not authorized or approved by ES&S, (b) use, modification, dismantling, disassembly, or transfer to third party without ES&S' prior written consent, (c) accident, theft, vandalism, neglect, abuse or use that is not in accordance with instructions or specifications furnished by ES&S, (d) causes beyond the reasonable control of ES&S or Customer, including acts of God, fire, flooding, riots, acts of war, terrorism or insurrection, government acts or orders; epidemics, pandemics or outbreak of communicable disease; quarantines; national or regional emergencies, labor disputes, transportation delays, governmental regulations and utility or communication interruptions, (e) Customer's failure to timely and properly install and use the most recent update provided to it by ES&S, or (f) Customer's failure to notify ES&S within three (3) business days after Customer knows of the need for such services. Any such Software License, Maintenance and Support shall be provided at the fees to be agreed upon by the parties if and when the need for such Software License, Maintenance and Support arises. Replacement versions of Software requested by Customer as a result of items set forth in this Section 3 or as a result of Customer's actions or inactions shall be billable to Customer at ES&S' then current rates.

4. **Proprietary Rights.** ES&S shall own the entire right, title, and interest in and to all corrections, programs, information, and work product conceived, created or developed, alone or with Customer or others, as a result of or related to the performance of this Agreement, including all proprietary rights therein or based thereon. Subject to the payment of all Software Maintenance Fees, ES&S hereby grants to Customer a non-exclusive license to use that portion of such corrections, programs, information, and work product that ES&S actually delivers to Customer pursuant to this Agreement. All licensed items shall be deemed to be ES&S Software for purposes of this Agreement. Except and to the extent expressly provided herein, ES&S does not grant to Customer any right, license, or other proprietary right, express or implied, in or to any corrections, programs, information, or work product covered by this Agreement.

5. **Reinstatement of Software License, Maintenance and Support.** If the Term expires without being renewed, Customer may thereafter receive a Software License and resume receiving Software Maintenance and Support upon (a) notification to ES&S, (b) payment of all fees, which would have been due to ES&S had the Term not expired, and (c) the granting to ES&S of access to the ES&S Software, so that ES&S may analyze it and perform such maintenance as may be necessary before resuming the Software License, Maintenance and Support Services.

## ARTICLE V
## MISCELLANEOUS

1. **Taxes; Interest.** Customer will provide ES&S with proof of its tax-exempt status. If Customer does not provide such proof, it shall pay, or shall reimburse ES&S for, all sales and use, excise or other similar taxes imposed on the transactions contemplated by this Agreement but shall in no event be liable for taxes imposed on or measured by ES&S' income. If Customer disputes the applicability of any tax to be paid pursuant to this Section 1, it shall pay the tax and may thereafter seek a refund. Any disputed or undisputed payment which is past due to ES&S will bear interest at the rate of one and one-half percent per month (or such lesser amount as may be permitted by applicable law) for each month or portion thereof during which it remains unpaid.

2. **Limitation of Liability.** Neither party shall be liable for any indirect, incidental, punitive, exemplary, special, or consequential damages of any kind whatsoever arising out of or relating to this Agreement. Neither party shall be liable for the other party's negligent or willful misconduct. ES&S' total liability to Customer arising out of or relating to this Agreement shall not exceed the aggregate amount to be paid to ES&S hereunder. By entering into this Agreement, Customer agrees to accept responsibility for (a) the selection of, use of and results obtained from any equipment, software or services not provided by ES&S and used with the Equipment or Software; or (b) user errors, voter errors or problems encountered by any individual in voting that are not otherwise a result of the failure of ES&S to perform. ES&S shall not be liable under this Agreement for any claim, damage, loss, judgment, penalty, cost, amount paid in settlement or fee that is caused by (y) Customer's failure to timely or properly install and use the most recent Update provided to it by ES&S or (z) Customer's election not to receive, or to terminate, the Hardware Maintenance Services or the Software License and Maintenance and Support.

3. **Excusable Nonperformance.** Except for obligations to make payments hereunder, if either party is delayed or prevented from performing its obligations under this Agreement as a result of any cause beyond its reasonable control, including acts of God, fire, riots, acts of war, terrorism or insurrection, government acts or orders; epidemics, pandemics or outbreak of communicable disease; quarantines; national or regional emergencies, labor disputes, transportation delays, governmental regulations and utility or communication interruptions, the delay shall be excused during the continuance of, and to the extent of, such cause, and the period of performance shall be extended to the extent necessary to allow performance after the cause of delay has been removed. ES&S agrees to work with Customer, at Customer's request, to develop mutually agreeable alternatives in order to minimize the negative impact of any such delay.

4. **Notice.** Any notice or other communication required or permitted hereunder shall be in writing and will be deemed given when (a) delivered personally, (b) sent by confirmed email, (c) sent by confirmed fax, (d) sent by commercial overnight courier (with written verification of receipt) or (e) sent by registered or certified mail, return receipt requested, postage prepaid, when the return receipt is received. All communications shall be sent to the attention of the persons listed on the signature page to this Agreement and at the addresses, email address or fax numbers set forth on such signature page unless other names, addresses or fax numbers are provided by either or both parties in accordance herewith.

5. **Assignment.** Except in the case of a reorganization of the assets or operations of ES&S with one or more affiliates of ES&S or the sale, transfer or assignment of all or substantially all of the assets of ES&S to a successor who has asserted its intent to continue the business of ES&S, neither party may assign or transfer this Agreement or assign, subcontract or delegate any of its rights, duties or obligations hereunder without the prior written consent of the other party hereto, such consent not to be unreasonably withheld or conditioned, nor unduly delayed.

6. **Entire Agreement.** This Agreement, including all exhibits hereto, shall be binding upon and inure to the benefit of the parties and their respective representatives, successors, and assigns. This Agreement, including Attachment 1 (which is specifically incorporated herein by this reference), contains the entire agreement of the parties with respect to the subject matter hereof and supersedes and replaces any and all other prior or contemporaneous discussions, negotiations, agreements or understandings between the parties, whether written or oral, regarding the subject matter hereof. Any provision of any purchase order, form or other agreement which conflicts with or is in addition to the provisions of this Agreement shall be of no force or effect. In the event of any conflict between a provision contained in an Attachment to this Agreement and these General Terms, the provision contained in the Attachment shall control. No waiver, amendment, or modification of any provision of this Agreement shall be effective unless in writing and signed by the party against whom such waiver, amendment or modification is sought to be enforced. No consent by either party to, or waiver of, a breach by either party shall constitute a consent to or waiver of any other different or subsequent breach by either party. This Agreement shall be governed by and construed in accordance with the laws of the State in which the Customer resides, without regard to its conflicts of laws principles. The parties agree that venue for any dispute or cause of action arising out of or related to this Agreement shall be in the state and federal courts of the United States located in the State in which the Customer resides. ES&S is providing Equipment, Software, and Services to Customer as an independent contractor, and shall not be deemed to be a "state actor" for purposes of 42 U.S.C. § 1983. ES&S may engage subcontractors to provide certain of the Equipment, Software, or Services, but shall remain fully responsible for such performance. The provisions of Article II, Section 1(f) and Article III, and Article IV, Sections 1-6 shall survive the termination of this Agreement, to the extent applicable.

7. **Counterparts; Execution By Facsimile.** This Agreement may be executed in two or more counterparts, each of which shall be deemed an original, but which together shall constitute one and the same instrument. The parties may execute this Agreement and exchange counterparts of the signature pages by means of facsimile transmission, and the receipt of such executed counterparts by facsimile transmission shall be binding on the parties. Following such exchange, the parties shall promptly exchange original versions of such signature pages.

IN WITNESS WHEREOF, this Agreement has been executed effective as of the date it is signed by the last of the parties hereto.

ELECTION SYSTEMS & SOFTWARE, LLC
11208 John Galt Boulevard
Omaha, NE 68137
Fax No.: 402-970-1291

DocuSigned by:
Jared Plath
D41BEDE76E434ED...
Signature

Jared Plath
Name (Printed or Typed)

V.P. of Finance
Title

8/29/2024
Date

ASHTABULA COUNTY, OHIO
8 W. Walnut Street
Jefferson, OH 44047
Fax No.: 440-576-1445

Signed by:
Kathryn Whittington
72C9CAC40E3D4A8...
Signature

Kathryn Whittington
Name (Printed or Typed)

Commissioner
Title

8/29/2024
Date

## PRICING SUMMARY AND PAYMENT TERMS

**Sale Summary:**

| Description | Refer To | Amount |
|---|---|---|
| ES&S Hardware Maintenance Fees | Attachment 1 | $123,350.00 |
| ES&S Software License, Maintenance and Support Fees | Attachment 1 | $131,080.00 |
| ES&S Firmware License, Maintenance and Support Fees | Attachment 1 | $77,910.00 |
| | | |
| **Total Maintenance Fees for the Term:** | | **$332,340.00** |

**Terms & Conditions:**

**Note 1**: Any applicable state and local taxes are not included and are the responsibility of Customer.

**Note 2**: **Invoicing and Payment Terms are as Follows:**

$66,468.00 due upon Contract Execution for the Coverage Period of March 1, 2024 through February 28, 2025.

$66,468.00 due on or before March 1, 2025 for the Coverage Period of March 1, 2025 through February 28, 2026.

$66,468.00 due on or before March 1, 2026 for the Coverage Period of March 1, 2026 through February 28, 2027.

$66,468.00 due on or before March 1, 2027 for the Coverage Period of March 1, 2027 through February 28, 2028.

$66,468.00 due on or before March 1, 2028 for the Coverage Period of March 1, 2028 through February 28, 2029.

**Attachment 1**

**ES&S HARDWARE MAINTENANCE DESCRIPTION AND FEES**

Term: **March 1, 2024 through February 28, 2029**

| Qty | Description | Coverage Period | Annual Maintenance Fee Per Unit | Maintenance Fee in Total |
|---|---|---|---|---|
| 73 | Model DS200 Scanner | 3/1/2024 through 2/28/2025 | $180.00 | $13,140.00 |
| 2 | Model DS450 Scanner | 3/1/2024 through 2/28/2025 | $2,314.00 | $4,628.00 |
| 58 | ExpressVote BMD | 3/1/2024 through 2/28/2025 | $119.00 | $6,902.00 |
| **Total Maintenance Fees for the Coverage Period March 1, 2024 through February 28, 2025** | | | [redacted] | **$24,670.00** |
| | | | | |
| 73 | Model DS200 Scanner | 3/1/2025 through 2/28/2026 | $180.00 | $13,140.00 |
| 2 | Model DS450 Scanner | 3/1/2025 through 2/28/2026 | $2,314.00 | $4,628.00 |
| 58 | ExpressVote BMD | 3/1/2025 through 2/28/2026 | $119.00 | $6,902.00 |
| **Total Maintenance Fees for the Coverage Period March 1, 2025 through February 28, 2026** | | | [redacted] | **$24,670.00** |
| | | | | |
| 73 | Model DS200 Scanner | 3/1/2026 through 2/28/2027 | $180.00 | $13,140.00 |
| 2 | Model DS450 Scanner | 3/1/2026 through 2/28/2027 | $2,314.00 | $4,628.00 |
| 58 | ExpressVote BMD | 3/1/2026 through 2/28/2027 | $119.00 | $6,902.00 |
| **Total Maintenance Fees for the Coverage Period March 1, 2026 through February 28, 2027** | | | [redacted] | **$24,670.00** |
| | | | | |
| 73 | Model DS200 Scanner | 3/1/2027 through 2/28/2028 | $180.00 | $13,140.00 |
| 2 | Model DS450 Scanner | 3/1/2027 through 2/28/2028 | $2,314.00 | $4,628.00 |
| 58 | ExpressVote BMD | 3/1/2027 through 2/28/2028 | $119.00 | $6,902.00 |
| **Total Maintenance Fees for the Coverage Period March 1, 2027 through February 28, 2028** | | | [redacted] | **$24,670.00** |
| | | | | |
| 73 | Model DS200 Scanner | 3/1/2028 through 2/28/2029 | $180.00 | $13,140.00 |
| 2 | Model DS450 Scanner | 3/1/2028 through 2/28/2029 | $2,314.00 | $4,628.00 |
| 58 | ExpressVote BMD | 3/1/2028 through 2/28/2029 | $119.00 | $6,902.00 |
| **Total Maintenance Fees for the Coverage Period March 1, 2028 through February 28, 2029** | | | [redacted] | **$24,670.00** |
| | | | | |

| Total Hardware Maintenance Fees for the Term | $123,350.00 |
|---|---|

**Note 1: The Per-Unit Fees if Customer requests more than one Routine Maintenance visit in a 24-month period shall be 75% of the then current maintenance fee per unit.**

**Note 2: Surcharge for Emergency Repair Services shall be the daily maintenance service rate in effect at the time such service is requested.**

**Note 3: Customer's Designated Location: Ashtabula County, Ohio**

**Note 4: The Per Unit Surcharge for performance of Routine Maintenance visit at more than one Customer Designated Location shall be $25.00 per unit for all units located at second or more locations.**

**Hardware Maintenance Services Provided by ES&S Under the Agreement**

1. Telephone Support.

2. Issue Resolution.

3. ES&S posts Technical Bulletins available through Customer's ES&S Web-based portal.

4. Routine Maintenance Services.

    - Onsite scheduled maintenance inspection per Article 2, Section 1a. The inspection includes:

        - Service performed by an ES&S trained and certified technician.

        - Performance of factory approved diagnostics on the unit, identifying and making adjustments where necessary as indicated by the testing.

        - Replacement of worn or defective with new or remanufactured federally and state certified parts.

        - Conducting a final test to verify that the unit is working according to manufacturer's specifications.

        - Use of a checklist tailored for each piece of equipment.

5. Repair Services.

    - Customer receives coverage for interim repair calls.

        - Interim calls may be scheduled during the regular Routine Maintenance Services event or scheduled in conjunction with other service work being performed in close proximity of Customer's location if they are not election critical.

        - A Product may be sent to ES&S' Depot location for repairs at a time to be mutually agreed upon by ES&S and Customer.

6. Priority Services.

    - Customer has access to the ES&S Help Desk for assistance.
    - The customer receives priority on service calls.

- The customer receives priority on response time.
- The customer receives priority on certified ES&S parts inventory.

**Note:** Except for those Hardware Maintenance Services specifically set forth herein, ES&S is under no obligation and shall not provide other Hardware Maintenance Services to the Customer unless previously agreed upon in writing by the parties.

**ES&S SOFTWARE LICENSE, MAINTENANCE AND SUPPORT DESCRIPTION AND FEES**
**SOFTWARE**

License and Maintenance Term: **March 1, 2024 through February 28, 2029**

Listed below is the Software and Fees for which Software License, Maintenance and Support will be provided:

| Qty | Description | Coverage Period | Software License, Maintenance and Support Fee in Total |
|---|---|---|---|
| 1 | ElectionWare Software – PYO Standard | 3/1/2024 through 2/28/2025 | $21,148.00 |
| 2 | Balotar Software with MRS and SRS Capability | 3/1/2024 through 2/28/2025 | $5,068.00 |
| **Total License, Maintenance and Support Fees for the Coverage Period March 1, 2024 through February 28, 2025** | | [redacted] | **$26,216.00** |
| | | | |
| 1 | ElectionWare Software – PYO Base Package | 3/1/2025 through 2/28/2026 | $21,148.00 |
| | Balotar Software with MRS and SRS Capability | 3/1/2025 through 2/28/2026 | $5,068.00 |
| **Total License, Maintenance and Support Fees for the Coverage Period March 1, 2025 through February 28, 2026** | | [redacted] | **$26,216.00** |
| | | | |
| 1 | ElectionWare Software – PYO Base Package | 3/1/2026 through 2/28/2027 | $21,148.00 |
| | Balotar Software with MRS and SRS Capability | 3/1/2026 through 2/28/2027 | $5,068.00 |
| **Total License, Maintenance and Support Fees for the Coverage Period March 1, 2026 through February 28, 2027** | | [redacted] | **$26,216.00** |
| | | | |
| 1 | ElectionWare Software – PYO Base Package | 3/1/2027 through 2/28/2028 | $21,148.00 |
| | Balotar Software with MRS and SRS Capability | 3/1/2027 through 2/28/2028 | $5,068.00 |
| **Total License, Maintenance and Support Fees for the Coverage Period March 1, 2027 through February 28, 2028** | | [redacted] | **$26,216.00** |
| | | | |
| 1 | ElectionWare Software – PYO Base Package | 3/1/2028 through 2/28/2029 | $21,148.00 |
| | Balotar Software with MRS and SRS Capability | 3/1/2028 through 2/28/2029 | $5,068.00 |
| **Total License, Maintenance and Support Fees for the Coverage Period March 1, 2028 through February 28, 2029** | | [redacted] | **$26,216.00** |
| | | | |
| **Total Software License, Maintenance and Support Fees for the Term** | | | **$131,080.00** |

**ES&S SOFTWARE LICENSE, MAINTENANCE AND SUPPORT DESCRIPTION AND FEES**
**FIRMWARE**

License and Maintenance Term: **March 1, 2024 through February 28, 2029**

Listed below are the Hardware Products and Fees for which Firmware License, Maintenance and Support will be provided:

| Qty | Description | Coverage Period | Annual Firmware License, Maintenance and Support Fee Per Unit | Firmware License, Maintenance and Support Fee in Total |
|---|---|---|---|---|
| 73 | Model DS200 Scanner | 3/1/2024 through 2/28/2025 | $98.00 | $7,154.00 |
| 2 | Model DS450 Scanner | 3/1/2024 through 2/28/2025 | $1,923.00 | $3,846.00 |
| 58 | ExpressVote BMD | 3/1/2024 through 2/28/2025 | $79.00 | $4,582.00 |
| **Total License, Maintenance and Support Fees for the Coverage Period March 1, 2024 through February 28, 2025** | | | [redacted] | **$15,582.00** |
| | | | | |
| 73 | Model DS200 Scanner | 3/1/2025 through 2/28/2026 | $98.00 | $7,154.00 |
| 2 | Model DS450 Scanner | 3/1/2025 through 2/28/2026 | $1,923.00 | $3,846.00 |
| 58 | ExpressVote BMD | 3/1/2025 through 2/28/2026 | $79.00 | $4,582.00 |
| **Total License, Maintenance and Support Fees for the Coverage Period March 1, 2025 through February 28, 2026** | | | [redacted] | **$15,582.00** |
| | | | | |
| 73 | Model DS200 Scanner | 3/1/2026 through 2/28/2027 | $98.00 | $7,154.00 |
| 2 | Model DS450 Scanner | 3/1/2026 through 2/28/2027 | $1,923.00 | $3,846.00 |
| 58 | ExpressVote BMD | 3/1/2026 through 2/28/2027 | $79.00 | $4,582.00 |
| **Total License, Maintenance and Support Fees for the Coverage Period March 1, 2026 through February 28, 2027** | | | [redacted] | **$15,582.00** |
| | | | | |
| 73 | Model DS200 Scanner | 3/1/2027 through 2/28/2028 | $98.00 | $7,154.00 |
| 2 | Model DS450 Scanner | 3/1/2027 through 2/28/2028 | $1,923.00 | $3,846.00 |
| 58 | ExpressVote BMD | 3/1/2027 through 2/28/2028 | $79.00 | $4,582.00 |
| **Total License, Maintenance and Support Fees for the Coverage Period March 1, 2027 through February 28, 2028** | | | [redacted] | **$15,582.00** |
| | | | | |
| 73 | Model DS200 Scanner | 3/1/2028 through 2/28/2029 | $98.00 | $7,154.00 |
| 2 | Model DS450 Scanner | 3/1/2028 through 2/28/2029 | $1,923.00 | $3,846.00 |
| 58 | ExpressVote BMD | 3/1/2028 through 2/28/2029 | $79.00 | $4,582.00 |
| **Total License, Maintenance and Support Fees for the Coverage Period March 1, 2028 through February 28, 2029** | | | [redacted] | **$15,582.00** |
| | | | | |

| Qty | Description | Coverage Period | Annual Firmware License, Maintenance and Support Fee Per Unit | Firmware License, Maintenance and Support Fee in Total |
|---|---|---|---|---|
| **Total Firmware License, Maintenance and Support Fees for the Term** | | | | **$77,910.00** |

**Software License, Maintenance and Support Services Provided by ES&S under the Agreement**

1. Telephone Support.

2. Issue Resolution.

3. Technical Bulletins will be available through Customer's ES&S Web-based portal.

**Note:** Except for those Software License, Maintenance and Support Services specifically set forth herein, ES&S is under no obligation and shall not provide other Software License, Maintenance and Support Services to the Customer unless previously agreed upon by the parties.

**Software License, Maintenance and Support and Hardware Maintenance and Support Services – Customer Responsibilities**

1. Customer shall have completed a full software training session for each product selected.

    - Customer shall have completed training at a proficiency level to successfully use the hardware (firmware) and software products.

    - Customer shall have the ability to install firmware and application software and make changes to date and time settings.

    - Customer shall have the ability to change consumable items. Any other changes made by the customer must be pre-approved in writing by ES&S.

2. Customer shall have reviewed a complete set of User Manuals.

3. Customer shall be responsible for the installation and integration of any third-party hardware or software application, or system purchased by the Customer, unless otherwise agreed upon, in writing, by the parties.

4. Customer shall be responsible for data extraction from Customer voter registration system.

5. Customer shall be responsible for implementation of any security protocols physical, network or otherwise which are necessary for the proper operation of the ES&S Equipment and ES&S Software.

6. Customer shall be responsible for the acceptance of the Equipment and Software, unless otherwise agreed upon, in writing, by the parties.

7. Customer shall be responsible for the design, layout, set up, administration, maintenance, or connectivity of the Customer's network.

8. Customer shall be responsible for the resolution of any errors associated with the Customer's network or other hardware and software not purchased or recommended by ES&S and not otherwise identified in the User Guides as part of ES&S' Equipment and Software.

9. Customer shall be responsible for all costs associated with diagnosing ballot printing problems resulting from the use of non-ES&S Ballot Partner Printers ballots.

10. Customer shall be responsible for the payment of additional or replacement Software CDs or DVDs requested by Customer. The price for such additional or replacement Software CDs or DVDs shall be at ES&S' then current rates.

# AMENDMENT

This Amendment to the Hardware Maintenance and Software License, Maintenance and Support Services Agreement ("Agreement") dated _____, 2024 is entered between Ashtabula County Board of County Commissioners on behalf of the Ashtabula County Board of Elections ("County") and Election Systems & Software, LLC ("Vendor"). The County and Vendor are sometimes collectively referred to herein as the "Parties" and individually as a "Party."

The Parties agree to the amend the Agreement as follows:

1. Vendor represents that it has sufficient training, expertise, staffing and experience to professionally provide the services as delineated in the Agreement and any exhibits attached thereto. Vendor represents and warrants to County that it will provide its services in compliance with all federal and state laws and regulations, including the security standards in the Ohio Secretary of State's Security Directives and the Election Official Manual. Vendor further represents and warrants to County that neither Vendor, in connection with performing the services in performance of this Agreement, nor the completed product delivered by Vendor, will infringe any patent, copyright, trademark, trade secret or other proprietary right of any person. Vendor further represents and warrants to County that it will not use any trade secrets or confidential or proprietary information owned by any third party in performing the services related to this Agreement or in delivery of the completed product unless Vendor has the authority to license, use or provide those trade secrets or confidential or proprietary information to County. Vendor further represents and warrants to County that neither Vendor nor any other company or individual performing services pursuant to this Agreement is under any obligation to assign or give any work done under this Agreement to any third party.
2. Vendor, at its own expense and regardless of any limitation on liability of any kind in this Agreement, shall defend and indemnify County against claims that products furnished under this Agreement infringe a United States patent or copyright or misappropriate trade secrets protected under United States law. As to any product which is subject to a claim of infringement or misappropriation, Vendor may (a) obtain the right of continued use of the product for County or (b) replace or modify the product to avoid the claim. If neither alternative is available on commercially reasonable terms then, at the request of Vendor, any applicable Software license and its charges will end, County will stop using the product, and will return the product to Vendor. Upon return of the product, Vendor will give County a credit for the price paid to Vendor, less a reasonable offset for use and obsolescence.

3. To the maximum extent permitted by law and regardless of any limitation on liability of any kind in this Agreement, the Vendor shall indemnify and hold harmless the County and the County's consultants, agents, and employees from and against all claims, damages, losses, and expenses—whether proven or not—including but not limited to attorneys' and consultants' fees—whether made by County or a third-party—arising out of or related to the Vendor's performance of the Goods including but not limited to the failure of the Vendor to perform its obligations under this Agreement, any claims for bodily injury, sickness, disease, or death or to injury to or destruction of or loss of use of real or personal property including the Goods itself, claims for additional storage and handling charges, liens against funds, claims related to the alleged failure of the Vendor to perform in accordance with this Agreement, and/or claims related to the removal, handling, or use of any hazardous materials. The County may set off amounts equal to any sums for which it is entitled to be indemnified from the amounts otherwise due the Vendor under this Agreement. Notwithstanding anything to the contrary in this Agreement, neither party shall be liable for any indirect, incidental, punitive, exemplary, special, or consequential damages of any kind whatsoever arising out of or relating to this Agreement. Neither party shall be liable for the other party's negligent or willful misconduct. Except for any direct loss to County for bodily injury, death, or damage to property of County caused by the negligence, intentional or willful misconduct, fraudulent act, recklessness, or other tortious conduct of Vendor or Vendor's employees or agents for which there shall be no limitation of liability, Vendor's total liability to County arising out of or relating to this Agreement shall not exceed the aggregate amount to be paid to Vendor hereunder.
4. The County's total liability under the Agreement shall be limited to the amount set forth in the Auditor's certificate accompanying the Agreement. Under no circumstances shall the elected officials, officers, employees, council members, or agents of the County be personally liable for any obligations or claims arising out of or related to this Agreement. No change or additional schedule to the Agreement shall be effective against the County without a new Auditor's certificate.
5. The Vendor shall maintain insurance as set forth below:

   (a) **General Liability Coverage.** Vendor shall maintain commercial general liability insurance with a limit of not less than $1,000,000 each occurrence.

   County and its employees shall be named as additional insureds with respect to all activities under this Agreement.

   (b) **Automobile Liability Coverage.** Vendor shall maintain automobile liability insurance with a limit of not less than $1,000,000 each accident. Such insurance shall include coverage for owned, hired and non-owned automobiles.

(c) **Workers' Compensation.** Vendor shall maintain workers' compensation coverage as required by Ohio law.

(d) **Cyber Liability and Security Insurance** Vendor shall maintain cyber liability and security insurance or equivalent insurance product(s), with minimum liability limits of not less than $5,000,000 and first party limits of not less than $1,000,000, that will provide, without cost to the Vendor or County, an immediate response in the event of a data breach, including meeting all notification obligations of Vendor and County and, in the event the Data Breach involves personal information as defined by Chapter 1347 of the Ohio Revised Code, provide free credit monitoring for any affected individual for a minimum period of one year.

Prior to the commencement of any work under this Agreement, Vendor shall furnish the County with properly executed certificates of insurance for all insurance required by this Agreement. Certificates of insurance shall provide that such insurance shall not be cancelled without 30 days' prior written notice to County. Vendor will replace certificates for any insurance expiring prior to completion of work under this Agreement.

6. If any dispute or difference of any kind (a "Dispute") arises between the Parties in connection with, or arising out of, this Agreement, the Vendor and County within 30 days shall attempt to settle such Dispute in the first instance through discussions. The designated representatives of Vendor and County shall promptly confer and exert their best efforts in good faith to reach a reasonable and equitable resolution of such Dispute. If the representatives are unable to resolve the Dispute within fifteen (15) Business Days, the Dispute shall be referred within two (2) Business Days of the lapse of the fifteen (15) Business Day period to the responsible senior management of each party for resolution. Neither party shall seek any other means of resolving any Dispute arising in connection with this Agreement until the responsible senior management of Parties have had at least an additional fifteen (15) Business Days to resolve the Dispute following referral of the Dispute to them. The Courts of Ashtabula County shall retain exclusive jurisdiction to resolve any disputes between the parties to the extent in which the parties cannot resolve their disputes within a reasonable amount of time. This agreement does not prohibit the parties from seeking mediation before litigation. During the pendency of any mediation or litigation the Parties shall continue to perform their obligations under this Agreement subject to Court Order. All questions regarding the validity, intention, or meaning of this Agreement or any modifications of it relating to the rights and obligations of the parties shall be construed and resolved under the laws of the State of Ohio.

7. Appendix A, the Ashtabula County Board of Elections Security Supplement (2022) as mutually negotiated between the parties is incorporated by reference as if fully set forth herein. In the event of any conflict or ambiguity between the terms and conditions of the

Agreement, this Amendment, and Appendix A, the following order of precedence shall apply: (a) Appendix A; (b) this Amendment; (c) the Agreement.

All other terms and conditions of the Agreement shall remain in full force and effect.

Agreed upon and accepted by:

ELECTION SYSTEMS & SOFTWARE, LLC

By: DocuSigned by: Jared Plath D41BFDF76F434FD...

Its: Jared Plath

Date: 8/29/2024

ASHTABULA COUNTY BOARD OF ELECTIONS

By: Signed by: Kathryn Whittington 72C9CAC40E3D4A8...

Its: Commissioner

Date: 8/29/2024

Approved as to Legal Form Only:

By: Signed by: Colleen M. O'Toole 6DE1E44EBC8C4A1...

Colleen M. O'Toole,
Ashtabula County Prosecutor

Date: 8/29/2024

**Appendix A**
**Security Supplement - 2022**
**Ashtabula County Board of Elections**

## I. Introduction

This security supplement establishes additional actions that the Ashtabula County Board of Elections ("BOE") requires of Election Systems & Software, LLC, ("Vendor") to employ to defend the security and integrity of the BOE infrastructure. Except as otherwise stated herein, all reports, notices, and disclosures required to be sent to the BOE, shall be emailed to **Ashtabul@OhioSoS.GOV**.

## II. Protection of Board of Elections' Data

A. All solutions shall operate at the *moderate level baseline* as defined in the current published version of National Institute of Standards and Technology ("NIST") CSF and CIS control framework for elections.

B. Vendor shall obtain an annual Audit that meets the American Institute of Certified Public Accountants ("AICPA") Statements on Standards for Attestation Engagements ("SSAE") No. 16, Service Organization Control 1 Type 2 and Service Organization Control 2 Type 2 of its TierPoint location. All Audits will be at the sole expense of Vendor and the results shall be provided to the BOE within 30 days of its completion each year upon request subject to non-disclosure agreements. At no cost to the BOE, Vendor shall immediately remedy any relevant critical or high risk findings identified in each Audit as they pertain to the Services.

C. "Sensitive Data" constitutes any type of computerized data that presents a high or moderate degree of risk if released or disclosed without authorization. There is a high degree of risk when unauthorized release or disclosure is contrary to a legally mandated confidentiality requirement. There may be a moderate risk and potentially a high risk in cases of information for which the BOE has discretion under the law to release data, particularly when the release shall be made only according to State of Ohio policy or procedure. The Sensitive Data may be certain types of personally identifiable information ("PII") that is also sensitive; such as medical information, social security numbers, financial account numbers, or data obtained from the Bureau of Motor Vehicles or other governmental entities. The computerized data may also contain other types of information not associated with a particular individual such as security and infrastructure records. To protect BOE data as described in this agreement, in addition to its other duties regarding BOE data, Vendor shall:

1. Adopt a written policy defining procedures for how Vendor shall detect, evaluate, and respond to adverse events that may indicate an incident or an attempt to attack or access BOE data or the infrastructure associated with BOE data. A written copy of this policy shall be

provided to the BOE at Ashtabul@OhioSoS.GOV and the Secretary of State's Office at VendorSecurity@OhioSOS.gov.

2. Maintain in confidence all Sensitive Data Vendor may obtain, maintain, process, or otherwise receive from or through the BOE in the course of this Agreement.

3. Use and permit employees, officers, agents, and independent contractors to only use any Sensitive Data received from the BOE solely for those purposes expressly contemplated by the Agreement.

4. Not sell, rent, lease, disclose, or permit employees, officers, agents, and independent contractors to sell, rent, lease, or disclose, any such Sensitive Data to any third party, except as expressly permitted under this Agreement or required by applicable law, regulation, or court order.

5. Take all commercially reasonable steps to:

i. Protect the confidentiality of Sensitive Data received from the BOE; and

ii. Establish and maintain physical, technical, and administrative safeguards to prevent unauthorized access by third parties to Sensitive Data received by Vendor from the BOE.

6. Provide access to Sensitive Data only to those individual employees, officers, agents, and Independent Contractors who require access to such information in connection with the performance of Vendor's obligations under this contract.

7. Upon request by the BOE, promptly destroy or return to the BOE, in a format mutually agreed upon, all Sensitive Data received from or through the BOE.

8. Cooperate with any attempt by the BOE to monitor Vendor's compliance with the foregoing obligations as reasonably requested by the BOE.

9. Notify the BOE of the location in which Vendor will be performing the work for this contract, and all the locations where BOE data will be stored.

10. Intentionally Omitted.

11. Comply with all existing State of Ohio and county data security policies, standards and procedures designed to ensure the following:

i. Security and confidentiality of Sensitive Data.

ii. Protection against anticipated threats or hazards to the security or integrity of Sensitive Data.

iii. Protection against the unauthorized access to, disclosure of, or use of Sensitive Data.

iv. Suggest and develop modifications to existing data security policies and procedures or draft new data security policies and procedures when gaps are identified.

12. All BOE data shall be stored and maintained within the United States of America unless expressly authorized in writing by the BOE.

## III. Vendor Electronic Mail

A. All Vendor email accounts shall utilize Domain-based Message Authentication, Reporting and Conformance ("DMARC") services. DMARC provides email owners the ability to protect their email from unauthorized use by verifying authenticity. A key component of DMARC is Domain Keys Identified Mail ("DKIM"). The purpose of implementing DMARC and DKIM is to protect domains from being used in business email compromise attacks, phishing emails, email scams and other cyber threat activities. Additional information regarding DMARC services can be found at: https://cyber.dhs.gov/bod/18-01/#introduction-to-email-authentication.

B. Vendor's email services shall utilize Sender Policy Framework ("SPF"). SPF can direct mail servers to reject mail not coming from a validated source.

C. Vendor email accounts, used by employees providing support to the BOE shall be using MultiFactor Authentication ("MFA"). Any MFA solution used must follow NIST 800-63B standards, and can be achieved by using smart cards, certificates, one time use password tokens or biometrics. MFA using text messaging or simple message service ("SMS") are not permitted.

## IV. Network Protection

A. Vendor shall implement a Security Information and Event Management ("SIEM") solution including SIEM software. Any device connected to Vendor's network containing BOE data shall be configured to produce logs of both allowed and denied traffic.

B. Vendor shall deploy network protection steps to ensure protection of any computers or servers used in direct support BOE data. Vendor's system and devices, at a minimum, shall be protected by a firewall segmenting BOE data from the corporate network. This firewall shall have intrusion prevention features enabled between all systems and the rest of the corporate network.

C. This firewall, along with the firewall used to protect the corporation from the internet, shall be configured using "least privilege" and "deny by default" methodology. Least privilege constitutes

that only authorized services intended to allow Vendor to provide services to the BOE may be configured on this firewall. Deny by default constitutes that all other services or devices not explicitly allowed shall be denied by the firewall.

D. All remote management of workstations and servers shall be performed using a secure virtual private network ("VPN") connection using MFA. Any MFA solution used must follow NIST 80063B standards, and can be achieved by using smart cards, certificates, one time use password tokens or biometrics. MFA using text messaging or SMS are not permitted.

E. All Vendor firewalls shall be configured to log both allowed and denied traffic. All logs from the firewall shall be sent to Vendor's SIEM software. Upon request of the BOE or the Secretary of State's Office, any log information shall be forwarded to the SOS provided BOE SIEM.

## V. Vulnerability Management and Application Security

Vendor shall implement a vulnerability management program that will identify all vulnerabilities. The vulnerability management program shall:

A. Perform scans on at least a weekly basis against Vendor's network using an automated tool. This tool shall be able to detect when new systems are added to the local network, or if the authorized systems have a new port or protocol activated that was not validated against the system baseline. Scanning shall occur on Vendor's internal network, along with any internet/external accessible networks.

B. Issue an automated alert to the Vendor identifying all vulnerabilities. Records that these scans have been performed and remediated shall be kept in accordance with a Vendor retention policy. All such records shall be retained for at least one year. The BOE or Secretary of State's Office may request these records at any time to ensure that Vendor maintains compliance with this provision.

C. On a weekly basis, all systems used to support the BOE shall be scanned using a Security Content Automation Protocol ("SCAP") compliant vulnerability scanner. A written copy of the vulnerability scanner report shall be provided, in a format specified by the BOE, to the BOE **Ashtabul@OhioSoS.GOV** and the Secretary of State's Office at VendorSecurity@OhioSOS.gov within 30 days of the execution of this Agreement.

D. Remediate critical and high vulnerabilities identified on Vendor systems used to support the BOE and shall promptly notify the BOE. Notification shall, at a minimum, be provided in the form of a formal communication via email to **Ashtabul@OhioSoS.GOV** and the Ohio Secretary of State Help Desk at Vulnerability@OhioSOS.gov. This disclosure shall also include a remediation plan that will allow for such critical and high vulnerabilities to be remediated in a timely manner:

1. "Critical" and "High" vulnerabilities, as defined by NIST's National Vulnerability Database ("NVD") Common Vulnerability Scoring System ("CVSS"), shall be remediated within 15 calendar days of initial detection.

2. All other vulnerabilities shall be remediated within 30 calendar days of initial detection.

E. If Vendor develops applications, they shall abide by the Secure Software Development Lifecycle to ensure application do not introduce risk into the organization. All applications shall comply with the BOE Application Security Policy.

F. Vendor shall implement a public facing vulnerability disclosure policy, displayed on the Vendor's website, and a process to remediate reported vulnerabilities in a timely period, i.e., less than 120 days of report. Reported vulnerabilities shall be disclosed to the BOE at **Ashtabul@OhioSoS.GOV** and the Secretary of State's Office at VendorSecurity@OhioSOS.gov within the first 30 days of the initial report. A written copy of this policy shall be provided to the BOE at **Ashtabul@OhioSoS.GOV** and the Secretary of State's Office at VendorSecurity@OhioSOS.gov within 30 days of the execution of this Agreement.

## VI. Whitelisting and Secure Baseline Images

A. Only authorized devices shall be connected to Vendor's network. Vendor shall ensure that device whitelisting is performed at the network switch level, or at a minimum verify that all unused network ports are disabled, and connected devices are authorized. "Port security," which prevents unauthorized devices from forwarding packets on the network, requires a managed switch. Network switch(s) shall log all port activity to Vendor's SIEM. Upon request of the BOE, any log information shall be forwarded to the BOE's SIEM.

B. All systems used by Vendor to support the BOE shall utilize secure baseline master images. These baseline images shall ensure that only required software is installed on the computer, and that those images are secure.

C. Vendor shall ensure that only permitted software is installed on any systems used to support the BOE. Application whitelisting shall be deployed on these systems in order to support this function. The whitelisting solution shall deny any program that is not explicitly allowed. This provides additional protection from malware and other harmful programs.

## VII. Access Control

A. Vendor shall limit the number of individuals assigned administrative access to computers and configure system access to remove default credential assignments. Vendor users shall not sign into accounts on a normal basis with administrative privileges on the workstations. Users with administrative privileges shall maintain two separate user accounts: a standard user account and an administrative account. The administrative account is to be only used for administrative actions. Accounts with administrative privileges shall only be used on a limited basis, and only when it is

required for system administrative functions. At no point in time shall an administrative account on a workstation also be used to access the internet.

B. Access control restrictions also constitute least privilege in accordance with Section IV herein, and strong passwords in accordance with Section X hereafter. All such restrictions shall be enforced for all devices or systems where authentication is performed; including but not limited to active directory, local accounts, service accounts, and remote access accounts.

C. All access control events shall be logged. All access control logs shall be sent to Vendor's SIEM. Upon request of the BOE or Secretary of State's Office, any log information shall be forwarded to the SOS provided BOE's SIEM.

## IX. Secure Channels for Remote Access

A. All remote access to Vendor's systems and networks, by Vendor, Vendor's vendors, independent contractors, or otherwise, shall use secure remote access technologies such as Transport Layer Security (TLS v1.2 or higher) or IPSEC. MFA is required and shall comply with the requirements set forth in Section X hereafter.

B. Shell based access to hosts or terminals shall use public key authentication or MFA, over a secure transport such as SSH. Telnet and other "cleartext" protocols are strictly prohibited.

C. All remote access solutions shall use a VPN with MFA authentication.

D. All remote access traffic shall be encrypted pursuant to the State of Ohio's data encryption standards and policies. These policies can be found at: https://das.ohio.gov/buying-andselling/policies.

E. All encryption systems shall comply with NIST Federal Information Processing Standard ("FIPS") 140-2.

F. All remote access sessions shall be logged and stored in a SIEM. BOE and the Secretary of State's Office may require that this log information also be forwarded to the SOS provided BOE SIEM.

## X. Strong Passwords/Passphrases and MFA

A. All users of Vendor's systems supporting BOE accounts shall utilize the following controls:

1. Each user shall have a unique username and password/passphrase.

2. Users are strictly prohibited from sharing passwords/passphrases or multi-factor authentication devices.

3. Passwords/passphrases shall be complex and comply with the following complexity requirements.

i. Be at least 15 characters in length.

ii. Contain three out of the following four items:

a. Number

b. Lower-case letter

c. Upper-case letter

d. Symbol

iii. Does not contain the user's name or username.

iv. Avoid using simple dictionary words without proper lengths or complexity. Passwords/passphrases should be generated from pass phrases or uncommon word associations. For example, "Buckeyes68!AreBlah".

iv. Simple letter substitution is NOT considered acceptable. For example, D1ct10n4ry is not a secure password.

4. Passwords/passphrases shall not be re-used across different applications. For example, your personal email account and your business email account passwords cannot match. Your LinkedIn password/passphrase should not match your Twitter password/passphrase. This reduces the effectiveness of a popular threat called "credential stuffing."

5. Password managers are an effective method of storing multiple passwords.

6. Passwords/Passphrases shall be encrypted while stored in a format prescribed under NIST 80053.

B. MFA shall be used for:

1. All accounts accessing or modifying voter registration data and election systems.

2. All email access for employees or contractors supporting the BOE.

3. All administrative access.

4. All remote access sessions.

C. Any multi-factor solution shall follow NIST 800-63b standards, and can be achieved by using smart cards, certificates, one time use passwords tokens, or biometrics. Examples of MFA that meets these requirements include Microsoft Azure MFA, YubiKey or Google Authenticator. MFA using text messaging or SMS are not permitted.

## XI. Wireless Device Security

A. If wireless networks are being used to support the BOE, such wireless networks shall leverage WPA2 or later with AES encryption. If pre-shared keys (passwords/passphrases) are preconfigured with wireless networks, the wireless passwords/passphrases shall be changed upon initial deployment and every three months or at any time prescribed by the BOE or the Secretary of State's Office. Wireless network names ("SSIDs") shall be hidden and shall not identify the product that they support or reference any board of elections or governmental activity.

B. Wireless access points should be updated when manufacturer or firmware updates are made available. At a minimum, Vendor shall check for firmware updates on a monthly basis. Wireless networks shall also be security secured with a firewall and intrusion detection system. All wireless access logs shall be sent to Vendor's SIEM. Upon request of the BOE or the Secretary of State's Office, any log information shall be forwarded to the BOE's SIEM.

## XII. Malware Management

A. Vendor shall have an endpoint security solution deployed on every workstation and network connected server supporting the BOE. At a minimum, this shall include:

1. Anti-malware to quarantine or delete malicious or suspicious files, rootkits, trojans and spyware.

2. Host passed firewall services, if you are not using the Windows Firewall.

3. Endpoint detection and response ("EDR") to intelligently identify and flag activity not covered by current malware signatures.

4. Centralized administrative console to set policy, deploy software and process alerts.

5. Automatic daily updates of all software components and signatures.

6. Root cause analysis with forensics to show how the infection occurred along with actions the malware took.

B. Any infected workstations and servers shall be immediately disconnected (unplugged) from the network, but remain powered on until forensically sound evidence capture is appropriately conducted and approved. Vendor shall immediately report the incident to the BOE. Notification

shall, at a minimum, be provided in the form of a formal communication via email to **Ashtabul@OhioSoS.GOV** and the Ohio Secretary of State Help Desk at SecurityEvent@OhioSOS.gov.

C. All endpoint security events shall be sent directly to Vendor's SIEM.

## XIII. Data Encryption

Pursuant to the State of Ohio's data encryption standards and policies, all data containing social security numbers or driver license numbers shall be encrypted at rest, while being transmitted across the network, or taken off-site via portable media. Secure transfers shall use compliant encryption algorithms that ensure data has not been altered in transit or at rest. At a minimum, this applies to voter registration data in electronic format that resides within Vendor's networks and systems.

These Encryption policies can be found at: https://das.ohio.gov/buying-and-selling/policies.

All Encryption systems shall comply with NIST FIPS 140-2. These FIPS 140-2 compliant systems are listed at: https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search.

## XV. Penetration and Controls Testing

A. BOE may, at any time, in its sole discretion, elect to perform or cause a Security and Data Protection Audit to be performed. This includes, but is not limited to, a thorough review of Vendor controls, security/privacy functions and procedures, data storage and encryption methods, backup/restoration processes, as well as security penetration testing and validation. The BOE or the Secretary of State's Office, upon the express request and authorization of the BOE acting on the BOE's behalf, may utilize a third-party entity to perform a Security and Data Protection Audit to demonstrate that all requirements are met.

B. Vendor shall engage in an annual penetration test. A full copy of the annual penetration test including all findings, and the Vendor's remediation plan for any findings shall be promptly provided to the BOE **Ashtabul@OhioSoS.GOV** and the Secretary of State's Office at VendorSecurity@OhioSOS.gov.

## XVI. Criminal Background Checks

A. Vendor shall conduct criminal background checks on all employees or contractors supporting the BOE data. Vendor shall attest that a background check has been completed and that no disqualifying criminal offenses have been committed.

B. "Sensitive services" constitutes those services that:

1. Require access to customer/consumer/agency employee information

2. Relate to the BOE's computer networks, information systems, databases, or secure facilities under circumstances that would permit modifications to such systems, or

3. Involve unsupervised access to secure facilities.

C. Vendor shall adopt and maintain a policy to review background checks and consider whether any convictions should bar employment. At the request of the BOE or the Secretary of State's Office, Vendor shall attest that Vendor maintains the policy.

**XVII. Physical Security**

A. Facility shall have video surveillance systems monitoring sensitive locations and all egress/ingress locations.

B. All computer systems shall be located in a secure location segmented from general locations where access is restricted to authorized parties whose role is to support said system.

C. Access to those locations shall be logged for historical tracking.

**XVIII. Supply Chain Risk**

A. Vendor should avoid known defects in software and hardware. Vendor should avoid third-party software components with known vulnerabilities when less vulnerable alternatives are available and will not compromise required functionality. Vendor shall favor components and providers exposed to higher standards of rigor from stringent assessments, have a record of fixing discovered vulnerabilities in a timely manner, which in turn allows them to maintain greater long-term stability.

B. Vendor shall not use any products from known hostile nation states, or any reseller of their products. Vendor should refer to the following U.S. Department of Commerce website link for a list of vendors that shall not be used: U.S. Department of Commerce. Use the search bar and type a company name to verify if that entity is on the "Entity List." Additionally, Vendor should refer to the following DHS Directive link (https://cyber.dhs.gov/directives/) to maintain awareness of any emergency directives or binding operational directive guidance that could impact vendors, thirdparty solutions, devices in use at BOE or within the BOE stakeholder base.

C. Vendor shall conduct an annual supply chain risk assessment that compliant with NIST 800-161. Assessments should be carried out by qualified personnel, independent of design and development. This written copy of this assessment shall be supplied to the BOE **Ashtabul@OhioSoS.GOV** and the Secretary of State's Office at VendorSecurity@OhioSOS.gov within 30 days of the execution of this Agreement.

D. Vendor shall publish and share all software and hardware bill of materials to BOE to account for cost and risk of devices. Additionally, Vendor shall maintain traceability and

provenance of software and hardware components. This written copy shall be supplied to the BOE **Ashtabul@OhioSoS.GOV** and the Secretary of State's Office at VendorSecurity@OhioSOS.gov within 30 days of the execution of this Agreement.

E. Vendor shall respond to any BOE and Secretary of State's Office issued guidance and timelines mandating review, response, and/or mitigation based on federal partner emergency directives, binding operational directives, or trusted third-party information sharing.

## XIX. Vendor Responsibilities Related to Reporting of Concerns, Issues, and Security/Privacy Issues

A. If, over the course of the contract, security or privacy issues arise, whether detected by the BOE, another third-party entity, or Vendor, that was not existing within an in-scope environment or service prior to the commencement of any contracted service associated with this contract, Vendor shall:

1. Notify BOE of the issue or acknowledge receipt of the issue within one (1) hour. Notification shall, at a minimum, be conveyed in the form of a formal communication via email to **Ashtabul@OhioSoS.GOV** and the Ohio Secretary of State Help Desk at SecurityEvent@OhioSOS.gov.

2. Within twenty-four (24) hours from the initial detection or communication of the issue from the BOE, present a potential exposure or issue assessment document to the BOE's account representative and the Secretary of State Chief Information Security Officer with a high-level assessment as to resolution actions and a plan.

3. Within four (4) calendar days, and upon direction from the BOE, implement, to the extent commercially reasonable, measures to minimize the BOE's exposure to the security or privacy issue until such time as the issue is resolved.

4. Upon approval from the BOE and the Secretary of State's Office, implement a permanent repair to the identified issue at Vendor's cost.

B. Actual or Attempted Access or Disclosure

If Vendor determines that there is any actual, attempted or suspected theft of, accidental disclosure of, loss of, or inability to account for any sensitive data by Vendor or any of its Subcontractors (collectively "Disclosure") and/or any unauthorized intrusions into Vendor's or any of its Subcontractor's facilities or secure systems (collectively "Intrusion"), Vendor shall immediately:

1. Notify BOE within one (1) hour of Vendor becoming aware of the unauthorized disclosure or intrusion. Notification shall, at a minimum, be conveyed in the form of a formal communication via email to **Ashtabul@OhioSoS.GOV** and the Ohio Secretary of State Help Desk at SecurityEvent@OhioSOS.gov.

2. Investigate and determine if an intrusion and/or disclosure has occurred.

3. Fully cooperate with the BOE and the Secretary of State's Office in estimating the effect of the disclosure or intrusion and fully cooperate to mitigate the consequences of the disclosure or intrusion.

4. Specify corrective action to be taken.

5. Take corrective action to prevent further disclosure and/or intrusion.

C. Unapproved Disclosures and Intrusions: Vendor Responsibilities

1. Vendor shall, as soon as is practical, make a report to the BOE and the Secretary of State's Office at VendorSecurity@OhioSOS.gov including details of the disclosure and/or intrusion and the corrective action Vendor has taken to prevent further disclosure and/or intrusion. In the event of a disclosure, Vendor shall cooperate fully with the BOE and the Secretary of State's Office to notify the affected persons as to the facts and circumstances of the disclosure of the sensitive data. Additionally, Vendor shall cooperate fully with all government regulatory agencies and/or law enforcement agencies that have jurisdiction to investigate a disclosure and/or any known or suspected criminal activity.

2. If over the course of delivering services to the BOE, under this statement of work for in-scope environments, Vendor becomes aware of an issue, or a potential issue that was not detected by security and privacy teams, Vendor shall notify the BOE within two (2) hours. Notification shall, at a minimum, be conveyed in the form of a formal communication via email to **Ashtabul@OhioSoS.GOV** and the Ohio Secretary of State Help Desk at SecurityEvent@OhioSOS.gov.

3. In the event of a conflict between the terms and conditions of the Agreement and provisions in this section pertaining to security scans and breaches, the notification requirement in this section shall not supersede any stricter requirements in the Agreement, which due to the nature of an active breach shall take precedence over this section. The BOE may elect to work with Vendor under mutually agreeable terms for those specific resolution services at that time or elect to address the disclosure and/or intrusion independent of Vendor.

4. If Vendor identifies a potential issue with maintaining an "as provided" BOE infrastructure element in accordance with a more stringent State of Ohio level security policy, Vendor shall identify and communicate the nature of the issue to the BOE **Ashtabul@OhioSoS.GOV** and the Secretary of State's Office at VendorSecurity@OhioSOS.gov, and, if possible, outline potential remedies.

D. Security Incident Reporting and Indemnification Requirements

1. Vendor shall immediately report any security incident as soon as it becomes aware of any such incident to BOE, the Secretary of State's Office, Multi-State Information Sharing and Analysis Center ("MS-ISAC") and the Cybersecurity and Infrastructure Security Agency ("CISA"). For the purposes of this document, "Security Incident" constitutes the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

2. In the case of an actual or suspected security incident that may have compromised Sensitive Data, Vendor shall notify the BOE **Ashtabul@OhioSoS.GOV** and the Secretary of State's Office at VendorSecurity@OhioSOS.gov in writing within one (1) hour of Vendor becoming aware of the breach. Notification shall, at a minimum, be provided in the form of a formal communication via email **Ashtabul@OhioSoS.GOV** and the Ohio Secretary of State Help Desk at SecurityEvent@OhioSOS.gov. Vendor is required to provide the best available information from the investigation.

3. Vendor shall fully cooperate with the BOE and the Secretary of State's Office to mitigate the consequences of an incident/suspected incident. This includes any use or disclosure of the Sensitive Data that is inconsistent with the terms of this contract and of which Vendor becomes aware, including but not limited to, any discovery of a use or disclosure that is not consistent with this contract by an employee, agent, or Subcontractor of Vendor.

4. Vendor shall give the BOE and the Secretary of State's Office full access to the details of the breach/suspected breach and assist the BOE in making any notifications to potentially affected people and organizations that the BOE deems necessary or appropriate.

5. Vendor shall document and provide incident reports for all such incidents/suspected incidents to the BOE **Ashtabul@OhioSoS.GOV** and the Secretary of State's Office at VendorSecurity@OhioSOS.gov. Vendor shall provide updates to incident reports until the investigation is complete. At a minimum, the incident/suspected incident reports will include:

i. Data elements involved, the extent of the data involved in the incident, and the identification of affected individuals, if applicable.

ii. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed BOE data, or to have been responsible for the incident.

iii. A description of where the BOE data is believed to have been improperly transmitted, sent, or utilized, if applicable.

iv. A description of the probable causes of the incident.

v. A description of the proposed plan for preventing similar future incidents, including ongoing risk remediation plan approval.

vi. Whether Vendor believes any federal, state or local laws requiring notifications to individuals are triggered.

E. In addition to any other liability under this contract related to Vendor's improper disclosure of BOE data, and regardless of any limitation on liability of any kind in this contract, Vendor shall be responsible for acquiring one year's identity theft protection service on behalf of any individual or entity whose Sensitive Data is compromised while it is in Vendor's possession. Such identity theft protection shall provide coverage from all three major credit reporting agencies and provide immediate notice through phone or email of attempts to access the individual's credit history through those services.

## XX. Regulatory Compliance

If Vendor is dealing with regulated data on behalf of the BOE, Vendor shall comply with all federal, state, and local laws and regulations.

## XXI. Compliance with Security Supplement

Vendor shall provide to the BOE **Ashtabul@OhioSoS.GOV** and the Secretary of State's Office at VendorSecurity@OhioSOS.gov artifacts demonstrating compliance with the provisions contained herein. To satisfy compliance, BOE requires Vendor to attest that all provisions are fully satisfied. These artifacts and attestation shall be provided to the BOE **Ashtabul@OhioSoS.GOV** and the Secretary of State's Office at VendorSecurity@OhioSOS.gov within 30 days of the execution of this Agreement.

## Elections Addendum

For Vendors engaged in elections related services, these Vendors shall also adhere to the following requirements:

## XXII. Department of Homeland Security Services

A. The BOE may request that the Department of Homeland Security ("DHS") perform assessments on any systems supporting elections. Any reports from such DHS assessments shall be shared with the BOE and the Ohio Secretary of State's Office.

B. Assessments that could be performed include, but are not limited to, the following:

1. **Physical Security Assessment:** Review the physical security in place at Vendor's offices or data centers supporting the BOE.

2. **Risk and Vulnerability Assessment:** This onsite assessment gathers data and "combines it with national threat and vulnerability information" to detect vulnerabilities in network security. After completing the assessment, DHS provides a final report with its findings and

recommendations for improving network security controls. This assessment shall be performed every two years, at least 30 days before any primary or general election

3. **Remote Penetration Testing:** DHS will perform a remote penetration test to help ensure that systems are secure.

4. **Validated Architecture Design Review:** This review is designed to develop a detailed representation of the communications and relationships between devices to identify anomalous communication flows. Following the review, a participating organization will receive a report that includes discoveries and recommendations for improving organizational operations and cybersecurity.

5. **Cyber Threat Hunt:** DHS will perform an in-depth review onsite to determine if a network compromise has occurred.

6. **Cyber Hygiene Scans:** DHS will perform a weekly cyber hygiene scan against all internet exposed systems, including your website and email systems.

7. **Phishing Campaign Assessment:** This assessment will how well employees recognize common phishing emails and being malicious and report them.

C. The CISA Election Infrastructure Security Resource Guide provides many resources that may be useful, available at Election Security Tools & Resources (cisecurity.org). One of the services available is the Cyber Resilience Review ("CRR"). The CRR measures and enhances the implementation of key cybersecurity capacities and capabilities of election organizations. This nontechnical assessment helps the assessed organization to develop an understanding of their operational resilience and ability to manage cyber risk to critical services during normal operations and times of operational stress or crisis. The deliverable for the CRR is a report with "options for consideration" to improve cybersecurity posture.

D. Vendor shall become a member of the Information Technology ISAC ("IT-ISAC") and the Election Infrastructure ISAC ("EI-ISAC"). An ISAC is a nonprofit organization that provides a central resource for gathering information on cyber threats to critical infrastructure. It also serves as a twoway information sharing mechanism between the private and public sectors.

E. If a BOE deploys an Albert intrusion detection device on Vendor's network(s) directly supporting the BOE, Vendor shall ensure that any alerts received by the Albert device are promptly forwarded to the BOE.

F. Depending on the severity of any security incident, images of the workstation may be collected and sent to the CISA for forensic investigation at the request of BOE or the Ohio Secretary of State's Office.