DATA Act Grant Funding Agreement

This Agreement is between the **Ohio Secretary of State** ("SOS") and the **Board of Elections of _____ County, Ohio** ("Board").

Background

The parties enter this Agreement with the following mutual understanding:

- On June 30, 2023, the General Assembly passed House Bill 33 (H.B. 33), and Governor Mike DeWine signed the bill into law on July 5, 2023.

- This act appropriates funds to be used by the SOS to provide financial assistance to county boards of elections to assist with the implementation of the Data Analysis Transparency Archive Act, including updating county voter registration systems.

Terms and Conditions

In consideration of the mutual benefits contained in this Agreement, the parties agree to the following terms and conditions.

Certification of Funds:
It is expressly understood and agreed by the parties that none of the rights, duties, and obligations described in this Agreement shall be binding on either party until all relevant statutory provisions of the Ohio Revised Code ("R.C."), including R.C. 126.07, have been complied with, and until such time as all necessary funds are available or encumbered and, when required, such expenditure of funds is approved by the Controlling Board of the State of Ohio, or in the event that funds are used, until such time that the SOS gives the Board written notice that such funds have been made available to the SOS by the SOS's funding source.

Distribution and Use of Funds:
Subject to the conditions below, the SOS will provide funding to the Board in an amount based on the cost of implementation of the changes with the county's selected election equipment vendor to help cover expenses associated with implementation of the DATA Act (the "DATA Act Funds"). The boards of elections must obtain an invoice from their Voter Registration vendors for the cost of the DATA Act implementation to include invoices for the Voter Registration system updates and one invoice for the Voter Registration Daily Snapshot.

As a condition of accepting the funds, the Board agrees to satisfy the terms and conditions herein and comply with any instructions or guidance from the SOS, including but not limited to the requirements of Directive 2024-18, or any other future Directives or guidance issued by the Secretary of State for the implementation of the DATA Act.

Upon receipt of the signed grant agreement and invoice(s) provided by the county's voter registration vendor, the Secretary of State's office will issue the board an initial check for the implementation of the required Voter Registration application changes and data standardization.

A second check will be issued at a later date for the implementation of the Voter Registration Daily Snapshot file when the county submits an invoice from their vendor for that milestone

Monitoring and Audits:
The SOS may request any additional information related to the funding at any time. The Board agrees to provide access to fund-related records upon the request of the SOS or any other authorized state agency.

Records Retention:
The Board will maintain accurate records of all expenses incurred related to the funds provided under this Agreement for a minimum of five years. If those records are relevant to litigation, claims, audits, negotiations, or other proceedings initiated prior to the end of that five-year period, the Board must retain the records until the final disposition of those proceedings or until the end of the five-year period, whichever is later.

Revocation of Funding:
The SOS may revoke the funding if the Board fails to comply with the terms of this Agreement. If the SOS revokes the funding provided under this Agreement, the Board must provide restitution to the SOS for the funds expended and return any unused funds within 30 days.

Executive Order 2022-02D. The Board represents, warrants, and certifies that the Board has read and understands Executive Order 2022-02D regarding the State of Ohio's prohibition of purchases from or investment in Russian institutions or companies. Specifically, the Board understands and agrees that:

> During the performance of the services described in this Agreement, the Board shall not perform any service, subcontract for any service, or purchase any goods to be used under this Agreement from any Russian institutions or companies, and the Board shall not perform any service or locate any SOS data within Russia.
>
> The State of Ohio reserves the right to recover any funds paid to the Board for purchases from a Russian institution or company in violation of this section.

Business with China. During the performance of the services described in this Agreement, the Board shall not perform any service, subcontract for any service, or purchase any goods to be used under this Agreement from any Chinese institutions or companies, and the Board shall not perform any service or locate any SOS data within China.

The State of Ohio reserves the right to recover any funds paid to the Board for purchases from a Chinese institution or company in violation of this section.

Vendor Contracts. Vendor contracts must comply with the requirements in Appendix A.

Successors and Assigns:
This Agreement is binding upon the SOS and the Board and their respective officers, directors, administrators, successors, and assigns.

The Board must sign and upload this agreement to the DATA Act SharePoint site, https://ohiosos.sharepoint.com/sites/boe/DATA%20Act/Forms/AllItems.aspx no later than August 28, 2024, unless extended by the SOS, in order to receive funding.

The parties have executed this Agreement by their duly authorized officers as of the last date indicated below, as evidenced by the following signatures:

_____	_____
Ohio Secretary of State Kimberly Burns Assistant Secretary of State	Date
_____	_____
Board of Elections Director	Date
_____	_____
Board of Elections Deputy Director	Board Chairperson (Chairperson's signature needed only if there is no Deputy Director)

Appendix A

VENDOR CONTRACTS

Vendor relationships are an important area where security risk mitigation needs to occur. In recent years there have been several prominent cyber events that showed the importance of ensuring entities are aware of the risk a vendor poses to their operations. Reflecting on these events, the Secretary of State's Office intends to ensure boards of elections are doing everything they can to protect themselves and account for vendor risk.

Board of elections must work with their statutory legal counsel, the county prosecutor, to include cybersecurity-related terms and conditions in all new contracts and upon renewal of contracts involving voter registration systems, electronic pollbooks, ballot on demand services, voting machines and systems, and information technology services (collectively, "technology services contracts"). Specifically, technology services contracts should include language to ensure that the vendor will comply with the security standards in the Ohio Secretary of State's Security Directives and the Election Official Manual. This should be in the form of a Security Supplement or a substantially similar addition to the main contract. A template for such terms and conditions was previously provided to counties and can be found here: https://www.ohiosos.gov/globalassets/elections/directives/2022/dir2022-38-2022-vendormanagementsecuritysupplementtemplate.pdf. Boards must involve their legal counsel, the county prosecutor, and technical points of contact in reviewing and negotiating technology services contracts.

The Security Supplement template includes standard cybersecurity related terms for boards and vendors to include in technology services contracts, not all of which will apply to every technology services contract. However, a strict prohibition on Products from Foreign Vendors Banned by the Federal Government applies to all contracts. A more detailed explanation of the Security Supplement is available in the Technical Document accompanying this Directive. At a high level, the Security Supplement includes provisions for all of the following:

- Data Protection;
- Network Protection;
- Vulnerability Management and Application Security;
- Access Control;
- Secure Channels for Remote Access;
- Strong Passwords and Multi-Factor Authentication (MFA);
- Incident Response Plan;
- Supply Chain Risk;
- Prohibition on Products from Foreign Vendors Banned by the Federal Government
- Software Bill of Materials; and
- Incident Reporting.