Wisconsin Elections Commission

212 East Washington Avenue | Third Floor | P.O. Box 7984 | Madison, WI 53707-7984
(608) 266-8005 | elections@wi.gov | elections.wi.gov

Election Security Subgrant Proposal
Appendix B
Subgrant Compliance Standards

I. Background

A. Securing state information systems is critical. Wisconsin residents rely on the state, counties, and municipalities to deliver services reliably and safely. Cyber-attacks are a continuous threat to the delivery of those services. The state needs your help to protect state systems and residents' information.

B. Cyber threats commonly focus on the weakest link within systems, primarily the people using those systems. This document provides basic guidelines to reduce risks and ensure fundamental cybersecurity standards. If you need help understanding these requirements, please call the WEC Help Desk.

C. Terms Defined.

Compliant Device: a device that meets minimum security standards outlined in II.A. below.

Managed Device: a device that is receiving managed service.

Managed Service: ongoing IT support meeting the requirements outlined in section II.B. below.

Managed Service Provider: a company offering managed service to customers; usually for a monthly fee.

II. Basic Guidelines for Appropriate Access to and Use of State Systems

A. Compliant Computer Hardware and Software that Meets the WisVote Policy Requirements.

Jurisdictions must use grant funds to meet this requirement before spending funds on any other need. The ES grant will allocate $600 for the purchase of one device by the jurisdiction. If you need help understanding these requirements, please call the WEC Help Desk. Compliant hardware and software must meet the following standards:

i) Computers using a currently supported operating system (OS).
   a. Windows 10 or Windows 8.1
   b. MacOS 10.14 Mojave (or newer)
   c. Consult with an IT professional or call the Elections Help Desk if you run another operating system (Linux, Chrome OS, etc.).

d. See Appendix C for information on how to check your Operating System.

ii) Computers with current:

a. Patches / Firmware (no later than 30 days of release by vendor). Ensuring your operating system is up-to-date will generally take care of this requirement. For smaller jurisdictions automatic updates will fulfill this requirement so long as they are not delayed or disabled.

b. Antivirus software.

c. Anti-spam and anti-spyware software.

d. Web filtering software to protect against malicious websites.

e. Merely possessing anti-malware software is not enough. You must download updates regularly to ensure your system is protected from the latest threats.

iii) Computers owned or controlled by the jurisdiction. While the WEC respects and permits remote work and work-from-home arrangements, jurisdictions must have at least one device that is under the jurisdiction's legal control to meet this baseline standard. This allows a jurisdiction to remain compliant in the event of staff turnover.

The WEC will install endpoint verification testing in WisVote to verify compliance upon login. Devices not in compliance by January 28, 2020 will be denied access to WisVote.

How to Achieve Compliance:

i) Purchase a Compliant Hardware Device. If a jurisdiction does not have compliant hardware or software/operating system it must use the ES Subgrant funds to achieve compliance. Local Election Jurisdictions may use their funds to purchase a compliant hardware device from vendors on the state contract or from any other vendor or local retail store they choose. More information regarding the purchase of compliant devices is included in Appendix C.

ii) Update Your Operating System to Windows 10. One option is to update the operating system on the computer currently used to access WisVote. For example, if the jurisdiction is currently using the Windows 7 operating system, and the computer and software are otherwise compliant, $200 of subgrant funds may be requested to upgrade the operating system. More information regarding updates to operating systems is included in Appendix C. Note that this option requires ongoing IT support to ensure systems stay current.

B. <u>IT Support Capable of Maintaining Minimum Standards</u>

Jurisdictions must certify that they are able to <u>maintain</u> their hardware and software in accordance with the policies above through 2022. This means that each jurisdiction must either possess professional, full-time IT staff, or obtain managed support through a managed support provider. The IT support must agree to maintain current patches, firmware, anti-virus software, and web filtering software. IT support must also notify the WEC of any cybersecurity incidents involving the jurisdiction's clerk or election systems, and

agree to receive Cyber Alerts from the Information Sharing and Analysis Center. More information on these requirements is provided in Appendix C. The ES grant will allocate $500 towards managed support costs that meet baseline standards. Jurisdictions must certify compliance by completing the WEC Security Subgrant Compliance Form, however the WEC will monitor the patch level of devices used to access WisVote. If a device is not in compliance with patching requirements, the WEC will follow up with the municipality to help achieve compliance. While the jurisdiction is awaiting a patch, the user may be denied access to WisVote until the patch is complete. If you need help understanding these requirements, please call the WEC Help Desk.

How to Achieve Compliance:

i) Obtain a Managed Service Provider. A jurisdiction may also use their ES grant funds to contract with a managed IT support provider to maintain minimum standards. The local election jurisdiction will then need to certify that it has compliant IT support and provide the documentation detailing their support with their Election Security Subgrant Compliance Form. More information about choosing a support provider is included in Appendix C.

ii) Possess in-house, shared, or contracted IT staff that provides all the services listed in Appendix C. The local election jurisdiction will then need to certify that it has compliant IT support and provide the documentation detailing their support with their Election Security Subgrant Compliance Form.

C. Complete WEC Election Security Training Requirements

(1) Participate in an Election Security Exercise

To comply with the terms of the ES Subgrant program, a representative from each local election jurisdiction must participate in an Elections Security TTX, Elections Administration TTX, Cyber Security Workshop, or Elections Security Roundtable before August 1, 2020. Jurisdictions may apply up to $100 of ES Subgrant funds to cover travel expenses and staff time associated with this requirement. The jurisdiction must certify their attendance at an event on the WEC Security Subgrant Compliance Form. Subgrant funds may be used for travel expenses and staff time associated with election security training. Attendance at a past training event will meet the requirements of this subgrant, however the $100 is only available for new attendance.

(2) Completion of WisVote Cyber Security Training

Upon acceptance of the ES Subgrant, the local election jurisdiction agrees to abide by the WisVote access policy. Regardless of whether the jurisdiction is a WisVote user or not, each full-time employee performing elections work must complete six free on-line training modules. If the jurisdiction is not currently using WisVote, it can request access to the WEC learning center and complete the required training by following the instructions in Appendix C. Completion of the training requires approximately 1.5 hours. Past completion of the training will meet the requirements of this subgrant.

D. Completion of a Contingency Plan

The WEC recommends every municipality maintain a contingency plan in the event of an election security crisis, and the completion of a plan is a requirement for the subgrant program. To assist with this process, information about preparing a sample contingency plan can be found in Appendix C.