Election Assistance Commission
Best Practices in Election Administration
2018 National Competition

Clearie Award Submission: Securing WisVote
Category: Outstanding Innovations

Submitted by:

The State of Wisconsin Elections Commission

212 East Washington Avenue, 3rd Floor

Madison, Wisconsin 53703

(608) 266-8005

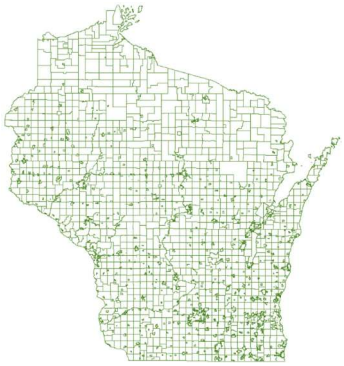
elections@wisconsin.gov

State of Wisconsin

The State of Wisconsin administers elections at the municipal level and is comprised of 1,852 municipalities. Each municipality's election data, e.g. voter registration, ballot access, ballot tracking, polling place, etc., is managed in a state-wide database called WisVote. The Wisconsin Elections Commission (WEC) developed WisVote for use at the state, county and municipal levels. Today there are over 2,500 WisVote users in the State of Wisconsin, each with varying computer skills, hardware configurations, and access to technical support.

Abstract

The responsibility of administering and conducting elections in over 1,800 municipalities comes with several challenges. The Wisconsin Elections Commission created, and continues to maintain, a state-wide voter registration database to assist municipalities in ensuring Wisconsin elections remain free, fair, and efficient. One substantial challenge, in Wisconsin and across the nation, is the obligation to ensure the data contained within election databases remains secure. The challenge is compounded as the number of database users increases.



The over 2,500 WisVote users possess varying computer skills and access to resources. Some users live and conduct elections in small townships with personally owned computers and limited technical support. Others serve in large cities with comprehensive information technology infrastructure. In addition, WisVote users also have different degrees of system permissions, from read-only to the ability to change and update election and voter data. Finally, many Wisconsin election officials also serve in other municipal or county capacities, municipal treasurer for instance, and are therefore likely have access to personally identifying information in their other roles.

Because the population of Wisconsin election officials is so varied, the WEC examined how we might establish a baseline level of computer security awareness for election officials across the State. After researching several commercial options, we concluded the most effective option was to create our own electronic learning modules, focused on cybersecurity best practices, and tailored for our considerable audience. The published training modules compose the "Securing WisVote" series.

Creating in-house interactive electronic learning modules offered several benefits, including:

- cybersecurity training tailored to our local county and municipal audiences;
- training housed on a learning center platform that the WEC staff controls;
- training that can be assigned and tracked by WEC staff;
- training that can be efficiently updated by WEC training staff;
- access to additional cybersecurity resources that accompany training modules to include a Personal Computer Security Checklist and WisVote Technology Standards.

The Challenge

The threat of computer hackers, bad actors, and human error will always be present, and those threats continue to evolve with future elections. As part of Wisconsin's efforts to keep our voter registration database secure, the challenge was to educate local election officials about

cybersecurity best practices and to establish a baseline of cybersecurity awareness to help ensure WisVote remains secure. In researching the interactions of other state agencies with local clerks, it became apparent that no other entity was providing comprehensive tools for basic cybersecurity hygiene. The WEC therefore chose to create a security training program from the ground up. Although we are one of Wisconsin's smallest state agencies, the WEC recognized that no other entity would provide this service statewide down to the local level. Creating a common cybersecurity program would protect the integrity of voter data and assist in safeguarding other, non-election, office processes.

The Innovation

After assessing various training options, the WEC training staff decided to create interactive electronic learning modules that address common cybersecurity best practices. Each module was specifically designed to address the needs our local clerk population.

The Wisconsin Elections Commission created the following modules that are available on our agency's Learning Center platform:

1. **Securing WisVote – The Basics**
   Provides an introduction and overview of cybersecurity basics and what is to come in the follow-up learning modules.

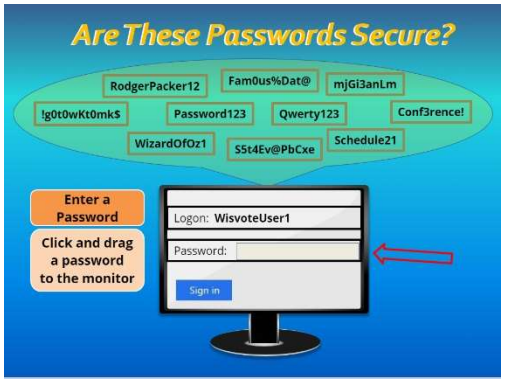
2. **WisVote Access Policy**
   Outlines the details of the new WisVote Access Policy, which was implemented in conjunction with the other modules, to help maintain the security of Wisconsin's voter registration database.

3. Phishing Facts

One of the most common forms of cybercrime. Phishing attacks are so simple that anyone with an email address can try it.

4. Password Protocols

Even with the very latest and greatest anti-virus software and the most powerful firewall, your passwords could be leaving you open to hackers and phishers. Today's sophisticated cybercriminals can exploit weak passwords in a matter of minutes. Take some time to strengthen yours.

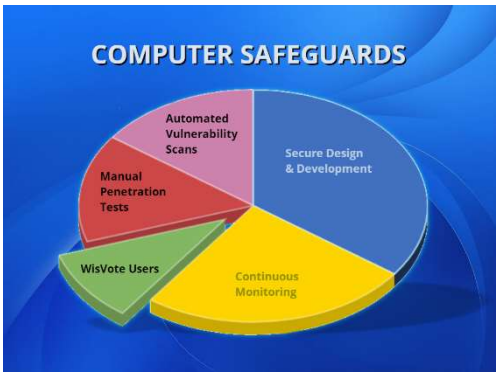


5. Browsing Safely

Modern internet browsers are packed with security features designed to stop you from visiting dodgy websites and to prevent sites from taking control of your computer. To make sure these features are always present and correct, and guarding against the latest threats, keep your browser software updated.

6. Computer Safeguards

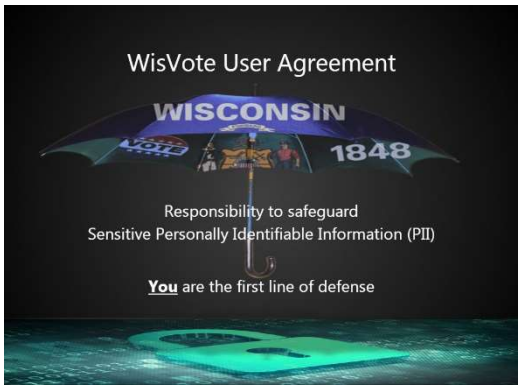
Safeguarding your computer requires protecting your hardware against damage or theft, protecting computer systems against malware and protecting valuable data from being accessed by unauthorized personnel or stolen by disgruntled staff. Physical security devices, security software, and data protection procedures should all be a part of your overall security plan.



Collectively, the modules make up the Securing WisVote series. The entire program is available to election workers at any level of government. While they are focused on election security, the modules provide cybersecurity best practices applicable to anyone safeguarding public information. Many clerks include these modules as part of their staff training.

To ensure compliance, the WEC created a WisVote User Agreement, and modified an existing Confidentiality Agreement, that requires completion of each cybersecurity module. This change afforded an opportunity to transition from paper to electronic agreements, thus eliminating the need for collection and retention of paper agreements.

The new policy consists of three requirements:



1. Completion of the Securing WisVote Series, a collection of six electronic learning modules available on the agency's electronic Learning Center platform;
2. Electronic (via WisVote) acknowledgement and acceptance of terms and conditions of the new WisVote Access Agreement; and
3. Electronic (via WisVote) acknowledgement and acceptance of terms and conditions of the updated WisVote Confidentiality Agreement.

Starting in 2018, all new WisVote users are required to complete cybersecurity training before WisVote credentials are issued. The user may then proceed to complete other training associated with the WisVote access level they require. Existing WisVote users are required to complete all cybersecurity training no later than December 31, 2018.

Efficacy

The Securing WisVote series represents a significant step towards enhanced cybersecurity at the local government level. While State agencies have long had access to professional IT support, not every municipal office is so fortunate. By creating a baseline training program open to all local governments, the WEC helped bridge cybersecurity awareness gaps within the WisVote user population. While the program is designed to safeguard the voter registration database, it has the added value of enhancing overall cybersecurity in local governments statewide.

Sustainability

The interactive electronic learning modules were created in-house by WEC training staff and are maintained and secured on state servers. Because the programs were created internally, the training modules can be easily updated or supplemented as needed. As our cybersecurity needs evolve, it is our intention to continue to add to this easily accessible library.

Outreach efforts

While this training is now mandatory in conjunction with the corresponding WisVote Access Policy, the electronic learning modules are accessible to any government officials or election

volunteers upon request. The WEC provided county and municipal level clerks access to the agency's Learning Center platform and encouraged the modules to be incorporated as part of election inspector training. We extended this opportunity to as many election officials as possible, helping them keep WisVote – and other electronic platforms – safe from cyberthreats. We've further offered elements of the program to other states, either as a model for their own program or for use as-is.

Cost-effectiveness

Electronic learning modules for cybersecurity awareness are available for purchase from outside vendors. The WEC staff researched several different costly options, generally based on the number of users. We determined creating a product in-house was most cost effective and allowed for sustained access to the content and integration with user records and permission within the statewide voter registration database. It also allowed us to create Wisconsin-specific content that resonates with our audience that could be easily improved based on user feedback.

Replicability

We believe these electronic learning modules could be replicated and tweaked to best fit the needs of any state. To that end, we have received request for access to the WEC Learning Center from numerous election officials and election security partners across the country interested in reviewing our product.

For the purpose of this application, an account was established on the WEC Learning Center Platform. To access the modules, please visit https://www.electiontraining.gab.wi.gov/ and sign in with the following credentials:

Username: **clearieaward**

Password: **MIwec2402!!**

After logging into the platform, click the **Election Security** Awareness tile to locate and access the individual learning modules.

Please note that upon announcement of award winners, this account will be disabled. Anyone wishing to have access to the leaning modules after that time may contact the Wisconsin Elections Commission.