



Municipal Clerks and Election Security

Reid Magney, Public Information Officer, Wisconsin Elections Commission

While most states run elections at the county level, Wisconsin's 1,850 municipal clerks have long been on the frontlines of administering our elections.

Whether they're registering voters, recruiting and training poll workers, establishing polling places, or counting votes, municipal clerks provide local service to voters in communities large and small in every corner of the state. They, along with the 72 county clerks, make up the most decentralized election administration system in America.

When it comes to election security, that decentralization can be both a strength and a weakness. Fortunately for the state and its voters, most municipal clerks have responded enthusiastically to the challenge, and are working closely with their county clerks to receive training and plan for safe, secure elections in 2020.

This article describes municipal clerks' role in election security and the Wisconsin Elections Commission's (WEC) efforts to make sure they have the resources and training they need for this very important mission to protect our voters and elections systems from hacking.

Even before election security became a buzzword a few years ago, municipal clerks were integrally involved in protecting the integrity of our elections. The tools and procedures they have used for decades to prevent old-fashioned election fraud like ballot-box stuffing also protect us from newer threats like hacking.

Wisconsin's focus on election cyber security intensified in 2017 with news that Russian hackers targeted Wisconsin and most other states in 2016 in some way. They were unable to access Wisconsin's systems due to the strong defenses provided to the WEC by the Wisconsin Division of Enterprise Technology.

However, that news caused the WEC to redouble its security planning efforts. While we were well protected by the state's firewalls from one kind of attack, we recognized that the statewide voter registration system could also be vulnerable if a local election official's access credentials were somehow compromised.

WEC adopted a multi-layered approach to protecting the statewide voter registration system, which WEC provides for

clerks to use for managing voter registrations and election data. The challenge of securing the system is compounded by the large number of users, many of whom are part time and do not have IT departments to support them.

Online Cybersecurity Training

The WEC's security team realized the importance of training local election officials in basic cyber hygiene practices to protect their systems and state systems from multiple threats including viruses, email phishing campaigns, and ransomware.

After researching several commercial options to provide cybersecurity training, the WEC concluded the most effective option was to create its own series of online learning modules focused on cybersecurity best practices, tailored for election officials across the state. By creating a baseline training program open to all local governments, the WEC helped bridge cybersecurity awareness gaps among system users and enhanced overall cybersecurity in local governments statewide.

WEC staff developed a series of six online training modules, known as Securing WisVote, and made them available to clerks on the agency's secure Learning Center website. Clerks who are users of the WisVote system are required to complete the training before gaining access.

WEC received an award in February 2019 from the U.S. Election Assistance Commission (EAC) for Outstanding Innovations in Elections for the Securing WisVote cybersecurity training program.

In-Person Cybersecurity Training

WEC also recognized the need to make sure clerks are prepared for an event that could disrupt an election, whether it came in the form of a cyberattack, a natural disaster like a flood or tornado, or even a terror attack.

In March 2018, WEC staff attended an election security training and tabletop exercise (TTX) hosted by the Defending Digital Democracy Project at Harvard Kennedy School of Government's Belfer Center in Boston. At the event, WEC staff worked with election officials and partners from across the United States to learn about election security best practices, as well as to participate in a TTX that simulated real-life security

related events that could potentially occur leading up to, and including, Election Day.

The WEC staff learned a great deal from the TTX and decided to adopt a similar model, focused on operational, physical, and cybersecurity, and tailored to the way we administer elections in Wisconsin.

WEC realized the importance of making that kind of training available to every municipal clerk in Wisconsin. WEC partnered with county clerks to help deliver the new training program throughout the state, starting in the spring of 2018. Since then, more than 1,500 local election officials have participated in the tabletop training exercises. WEC staff recently launched TTX 2.0 with a new set of scenarios and challenges designed to help clerks get ready for 2020.

In response to clerk suggestions, WEC has also recently developed new election security communications training exercises for municipal and county clerks. Clerks can view a webinar online and attend in-person communications training exercises being offered around the state. The training is based on a media toolkit the WEC developed for clerks, which provides sample news releases and holding statements for a variety of potential election security scenarios.

Technology - State

In addition to creating several kinds of cybersecurity training for local election officials, WEC has taken extraordinary steps to enhance the security of its systems by working closely with its technology and law enforcement partners in state and federal government. These steps include:

- Encrypting data on WEC servers and between the servers and users, so in the unlikely event of a breach, any data stolen would be unusable.
- Instituting a new system access policy requiring all users to complete the award-winning online training series. New users must complete security training before gaining access to the system and existing users were required to complete the training prior to the November 2018 election.
- Implementing Multi-Factor Authentication (MFA) for system access before the November 2018 General Election. All WisVote users must now use a third identification factor, in addition to their username and password, to gain access to the system. This involved providing nearly 3,000 WisVote users – mostly municipal clerks and their staffs – with FIDO security keys and training on the new MFA system.
- Upgrading existing monitoring tools to alert staff of any suspicious activity within the system.

- Redesigning reports that clerks can save and print from WisVote so they do not contain confidential information, such as voters' dates of birth and driver's license numbers.
- Completing risk, vulnerability, and penetration assessments in conjunction with U.S. Department Homeland Security and the Wisconsin Department of Administration – Division of Enterprise Technology (DET). The assessment found no evidence of any unauthorized access to Wisconsin's elections systems.
- Implementing an endpoint testing program, which requires users of WisVote to install a small program on their computers. When users access WisVote, the endpoint testing program reports on whether the computer's operating system and antivirus programs are up to date and secure. WisVote users must have up to date systems by January 28, 2020.

Technology - Local

In 2019, WEC has focused on making sure all municipal clerks have the technology and support they need to securely serve their voters. The commission approved a \$1.1 million Election Security Subgrant Program using federal election security funds. The program is designed primarily to help small municipalities where clerks were using outdated computers or their own personal computers to conduct official business, and where clerks do not have professional IT support.

Clerks could apply for up to \$1,200 to cover the costs of purchasing a computer, contracting for professional IT support services, and attending in-person election security training. The final numbers are still coming in, but the WEC processed 830 subgrant applications and has approved payments to approximately 664 towns, 115 villages, 46 cities, and five counties. Of the \$1.1 million originally allocated, approximately \$813,500 will be disbursed in this round of funding. Grants were distributed to every corner of the state in 71 out of 72 counties.

Though the November 15 deadline to apply for grants has passed, WEC is studying additional clerk security needs to allocate the remaining federal grant funds. Clerks have already been surveyed about their additional security needs, and the endpoint testing program, mentioned above, will help provide WEC staff with information about those needs. Possibilities include providing emergency technology grants to municipalities, especially those where a new municipal clerk comes into office and finds substandard technology resources.

WEC will also be working with clerks to help them get secure email addresses that have the @wi.gov domain. Many

municipalities use email domains that end in .com or .org, which could be vulnerable to impersonation.

Public trust in information provided by local election officials is important in all public communications – including information provided via email and local county and municipal websites. Many clerks are currently using Google, Yahoo, Hotmail, and other free email domains to communicate with voters. Free email services generally do not employ robust malware scanning features that would be an additional layer of security for clerks. In addition to the risk of malware or ransomware attacks, a bad actor could easily obtain an email domain designed to trick the recipient that it is from a government entity, allowing them to send disinformation that may cause disruption in the election process. This is because only the .gov domain is regulated by law. Other domains, such as .com, .org, and even .us are freely available to anyone willing to pay for them.

Municipal Clerk Election Security Responsibilities

This is a partial list of the important things municipal clerks do to ensure Wisconsin elections are secure:

- Municipal clerks are responsible for voter registration, which requires a majority of them have computer access to the Wisconsin's voter registration system. Larger municipalities generally handle entering and maintaining voter registration records in the system. Many smaller municipalities have what are known as relier agreements with their county clerks or a neighboring municipal clerk to enter records in the state's system.

- Municipal clerks receive electronic notifications from the state when there are new online registrations through the MyVote Wisconsin website, as well as requests for absentee ballots from voters at home, living overseas, and serving in the military.
- State law places responsibility for purchasing voting equipment on municipalities. To ensure continuity and compatibility, many municipalities work with their county clerks to coordinate purchasing and upgrading their voting equipment. Some counties share voting equipment costs with their cities, villages, and towns.
- Municipal clerks are responsible for training election inspectors (poll workers) in proper security procedures for ballots and voting equipment, including checking security seals and maintaining chain-of-custody records.
- Many municipal clerks provide secure storage facilities for voting equipment when it is not in use.
- Many municipal clerks provide secure storage for ballots and other election materials until they can be legally destroyed 22 months after a federal election.

About the Author:

Reid Magney is public information officer for the Wisconsin Elections Commission. He joined state service in 2009 after a 25-year career in journalism, including 14 years at the *La Crosse Tribune*, covering government, politics, and elections. You can reach him at reid.magney@wi.gov



Batterman
engineers surveyors planners

2857 Bartells Drive
Beloit, Wisconsin 53511
608.365.4464
www.rhbatterman.com



Excellence in Engineering
Since 1946.

Madison 608.251.4843
Milwaukee 414.271.0771
www.strand.com



DELTA 3
EVERY ANGLE COVERED

Professional Civil, Municipal & Structural Engineering
Architecture • Grant Writing • Land Development • Planning & CADD Services
Phone: (608) 348-5355 ▲ Website: www.delta3eng.com ▲ Platteville, WI



- Municipal Engineering
- Cross Connection Inspection
- Building Inspection
- Funding Procurement
- Project Management
- Planning & Design

920-356-9447
107 Parallel St.
Beaver Dam, WI 53916
www.kunkelengineering.com




PAA

- ◆ Executive Search/Selection
- ◆ Interim Management
- ◆ Compensation Plans
- ◆ Fire and Emergency Services Studies
- ◆ Strategic Planning/Organizational Audits

public-administration.com
paassoc@northnet.net
262-903-9509

PUBLIC ADMINISTRATION ASSOCIATES, LLC
Kevin Brunner David Bretl Dr. Stephen Hintz



Madison (608) 273-3350
Rhineland (715) 420-0579
Kenosha (262) 925-3210
www.tcengineers.net

CREATIVE SOLUTIONS FOR YOUR COMMUNITY SINCE 1981
water/wastewater • stormwater • municipal • GIS/mapping