Testimony of Richard Rydecki
Wisconsin Elections Commission

Assembly Committee on Science and Technology
March 28, 2018

Room 400 Northeast, State Capitol
Public Hearing

Chairperson Quinn and Committee Members:

Thank you for the invitation to provide testimony on behalf of the Wisconsin Elections Commission (WEC) regarding security procedures for state information technology. I am presenting this testimony on behalf of Interim Administrator Meagan Wolfe, who is in Boston this week to participate in training related to election security tabletop exercises.

The WEC is strongly committed to protecting Wisconsin electors' confidential information and has been working on the frontlines of cyber security with our partners at the Division of Enterprise Technology and Homeland Security to ensure the integrity of Wisconsin elections.

In this testimony, I will discuss:

- Types of voter data under the responsibility of the WEC
- IT applications developed by the WEC and how we work with DET on security monitoring
- WEC in-house security procedures and plans
- Existing and upcoming security training WEC provides to local election officials who use our IT applications.

Much of the information that the WEC collects and stores about Wisconsin voters is public information under state statutes. This includes the names, addresses and voting histories of more than 3 million currently registered voters, as well as millions of inactive voters. It may also include telephone numbers and email addresses of voters who chose to provide this optional information when they registered to vote.

The reason that basic information about voters is public is to provide transparency and accountability in the election process. For this reason, statutes and administrative rules require the WEC to make data from the statewide voter list available for purchase by the public, the parties, candidates and the media. The WEC has a website, https://badgervoters.wi.gov, where customers can purchase public voter information.

In addition to public information about voters, the Elections Commission also collects and maintains personally identifying information associated with each voter record that by statute cannot be provided to anyone other than election officials and law enforcement officers. This confidential information includes the voter's date of birth, driver license or state ID card number, the last four digits of the voter's Social Security number and information about whether the voter has requested an accommodation at the polling place because of a disability.

Wisconsin also has a confidential voter program designed to protect information about persons who are victims of sexual assault, domestic violence and abuse, and stalking. Voters who qualify for this program will not be listed on the section of the poll book available for public inspection and their information is excluded from data requests. These voters also are not publicly searchable on our MyVote Wisconsin voter information website.

The tool Wisconsin election officials use to track and maintain voter data is the statewide voter registration system. The state's first SVRS was launched in 2006, with the assistance of a vendor. In early 2016, a new platform was launched known as WisVote, which was built by our staff with the assistance of a small team of dedicated in-house IT contractors. The multi-year, multimillion dollar upgrade of the system was classified as a major IT project for the State.

WisVote is built on Microsoft Dynamics CRM, an enterprise-grade internet-based customer relationship management platform used by many Fortune 500 companies. Unlike many states which implemented voter registration systems developed by vendors, our team customized Microsoft Dynamics CRM to meet the needs of the state and local election officials in our unique decentralized system and the Commission purchases user licenses for each county and municipal clerk's office.

The Department of Administration's Division of Enterprise Technology (DET) provides the servers on which WisVote runs, as well as the data center and security systems that protect WisVote from intrusions. At the enterprise level, DET routinely detects and repels millions of scanning attempts against state IT systems each year and reports suspicious activity to federal authorities, who share that information so other states and can take appropriate protective steps. DET also provides secure, off-site back-ups for our data. The WEC is responsible for security at the application level, and continuously maintains the system, install patches, and develops new functionalities of the system.

Users of the WisVote system only have access to voter records within their jurisdiction. That way, if an individual clerk's access credentials were stolen, the potential damage that could be done would be limited. The system keeps audit logs of every action a user takes in the system, permitting administrators to restore any unauthorized changes from backup data. We are currently developing tools to analyze audit logs to identify potentially suspicious activity in the system and alert system administrators.

As the WEC continues to implement elections security best practices into its own election administration applications, one of our main initiatives is updating the policy and process in which users access the WisVote system. Currently, all WisVote users are required to submit a signed confidentiality agreement and a user policy agreement to the WEC before they are given access to the system. The updated confidentiality and user agreement will be housed electronically so that WEC staff can easily monitor compliance and submission of the agreement. WEC will begin rolling out the new policy and WisVote user requirements in May 2018 for new users and will require all existing users to acknowledge and comply with the new agreement by July 2018.

- The new agreement requires potential new WisVote users to complete WEC cyber security training before they will be given access to the user policy and assigned credentials to access the system. Security training is housed in the WEC online learning center. Once the training is complete and the user acknowledges the agreements, they will be given permissions to log into WisVote. Potential users will not be granted access to the system until they have completed the required training.
- The new policy reinforces the concept that users of the WisVote system are the custodians of Personal Identifiable Information (PII) for voters in their jurisdiction. The policy explains that as the custodians of PII, users of WisVote have a duty to operate election systems in a secure way by maintaining minimum system requirements, protecting their passwords, and utilizing other security best practices.
- The new policy requires that WisVote users keep the device used to access WisVote updated with current operating systems and patches.
- Users of WisVote will be required to report any election-related security issues or incidents to the WEC and appropriate law enforcement. If a WisVote user becomes aware of an issue or incident that could impact the WisVote system or voter data, they will be required to follow the WEC prescribed communications protocol in order to mitigate and/or remedy the issue.
- Language that allows the WEC and other government partners such as DHS and DET to conduct system testing and assessments is included in the new policy. This will allow WEC to arrange assessments, like the DHS phishing assessment, without having to get special authorization from each WisVote user every time a test or assessment is conducted.

WEC staff has also started the process of providing election security training to municipal and county clerks and is taking a unique approach compared to other state election offices. Almost all other states have a county-based election administration system and the state elections office is charged with training between 50 and 80 county offices on election security. In Wisconsin, the municipal-based election system requires the WEC to be responsible for training 1,853 municipal clerks and 72 county clerks about election security.

To the best of our knowledge, no other State agency has taken on the task of providing a basic level of cybersecurity and cyber hygiene training to local clerks, especially municipal clerks who have no in-house IT support. Few people would expect that it has fallen to the state's elections agency, one of the smallest state agencies, to ensure a base level of IT competence among local clerks in today's cyber environment.

The sheer number of local election officials in Wisconsin demands that the WEC deploy a variety of training methods, such as using the WisVote online learning center to provide interactive online training content and partnering with county clerks to develop a train-the-trainer elections security program for municipalities.

Using the online learning center, WEC staff has been able to develop six interactive online tutorials on various election security topics. These tutorials focus not only on election-specific training but also incorporate general cyber security best practices. These tutorials include: password security, avoiding phishing scams, avoiding ransomware and other malware, web browser security, and WisVote user policies. WEC will also incorporate other tools into the learning center such as checklists and links to additional training available through both the federal government and other national elections security groups.

In addition to online resources and preparations, WEC staff is also creating a partnership with the county clerks on an elections security training plan designed to provide in-person training to the municipal clerks on elections security and responding to cyber incidents. The goal is for counties to serve as regional hubs to train their municipalities and host additional regional trainings for election officials from neighboring counties. WEC staff will be meeting with county trainers to provide them with training materials, and train them on election security best practices, election security response plans and information on how to conduct table top exercises.

WEC staff has begun work on scheduling the trainings with the county clerks and developing the training materials. The plan is to coordinate training events for the county clerks on a schedule that will be completed by late April. The counties will then be expected to train the municipal clerks in the month of May. This will give municipalities time to implement security best practices and response and contingency planning into their election administration plans for the August and November elections.

In October 2016, the WEC issued its first Contingency Planning and Election System Security Report, which is available on the agency's website: http://elections.wi.gov/publications/manuals/contingency-planning-and-election-system-security-report. The report compiled and organized information regarding agency planning as well as recommendations and best practices for local election officials.

In 2017, the agency began working on a comprehensive, three-part update to that plan, known as the 2018 Wisconsin Elections Security Report, which will have three main sections: planning and preparation, response planning and communications.

A draft of the planning and preparation section of the document was completed in December 2018. WEC staff continues to build on that section of the report as new information and resources become available. Staff is also working on the response and communications section of the report by utilizing newly available resources from national partners. These resources are being used to develop Wisconsin-specific election security response plans for use by municipal and county clerks.

The response planning portion of the final report will outline potential election security scenarios and provide county and municipal clerks with suggested response plans. Scenarios will include potential incidents such as a compromised user password allowing unauthorized access to municipal voter lists, mitigating and responding to a ransomware or other malware attack, and attempted physical tampering with voting equipment.

The WEC will then develop response and communication plans and will assign each possible scenario to a response and communication plan that the clerk can reference in the event of such an incident. The response plans will include step-by-step guides, outline roles and responsibilities, and provide contacts for handling each scenario.

The communication plans will include a protocol for communicating such incidents to make sure that all necessary parties such as law enforcement, DHS, WEC and others are notified and involved in responding when appropriate.

The Wisconsin Elections Commission prioritizes its unique responsibility to protect the confidential data of millions of Wisconsin voters while also managing and providing access to this data for a diverse set of users across the state. Our desire to protect this data has necessitated and benefitted from the development of a strong partnership between our agency and the Division of Enterprise Technology, the Division of Emergency Management, and the National Guard. We have also worked with federal agencies, such as the Department of Homeland Security, to access security services that they provide.

Through this work with agency partners, we have been able to protect our confidential voter data on the state level. The protection of this data also relies upon the behavior of our system users on the county and municipal level, and the WEC is committed to providing and expanding relevant and effective election security training to these local election officials.

Respectfully submitted,

Richard Rydecki, Elections Supervisor
Wisconsin Elections Commission
608-261-2015/richard.rydecki@wi.gov