

Election Security Report

Wisconsin Elections Commission



September 2019

WISCONSIN ELECTIONS SECURITY PLANNING - 2019

Section I: Election Security Preparation and Incident Prevention

- A. (Page 1) U.S. Government Level** - Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), *U.S. Elections Assistance Commission (EAC)*, *Federal Voting Assistance Program (FVAP)*, and other federal agencies
1. (Page 2) [Certification of Voting Equipment \(EAC\)](#)
 2. (Page 2) *Providing Security Best Practices (EAC and DHS)*
 - a. (Page 3) [EAC - Managing Election Technology Documents](#)
 - i. (Page 3) [Ten Things to Know About Selecting a Voting System](#)
 - ii. (Page 4) [Ten Things to Know About Managing an Aging Voting System](#)
 - iii. (Page 4) [Considerations for Implementing Voting Systems with COTS Products](#)
 - iv. (Page 4) [Checklist - Securing Voter Registration Data](#)
 - v. (page 5) [Checklist - Securing Election Night Reporting Systems](#)
 - b. (page 6) DHS Resources and Best Practices
 - i. (Page 6) [Security Tips for Securing Voter Registration Data](#)
 - ii. (Page 7) [Best Practices for Continuity of Operations \(Handling Destructive Malware\)](#)
 - iii. (Page 7) Ransomware: What It Is and What to Do about It
 3. (Page 8) *Training for State and Local Governments*
 - a. (Page 8) Training Resources
 - i. (Page 8) [FEDVTE](#) (DHS)
 - ii. (Page 8) [US Cert](#) (DHS)
 - iii. (Page 9) [On GuardOnline](#) (Federal Trade Commission)
 - iv. (Page 9) [Stay Safe Online](#) (National Cyber Security Alliance)
 - v. (Page 9) [Stop. Think. Connect.](#) (National Cyber Security Alliance)
 - b. (Page 9) EAC In-person Trainings for Local Election Officials
 - i. (Page 10) DHS TTX events
 - ii. (Page 10) DHS Poster Guide for Local Elections Officials
 4. (Page 11) *Critical Infrastructure Designation & Monitoring Activity (DHS and FBI)*
 - a. (Page 11) Defining the Designation for Wisconsin
 - b. (Page 11) Coordinating Council
 - c. (Page 11) Providing Regular Scans
 - d. (Page 12) Risk Vulnerability Assessment (DHS)
 - e. (Page 12) EAC Resources
 - i. (Page 12) [Elections Critical Infrastructure Hub and Glossary](#)
 - ii. (Page 13) [CI Scoop Blog](#)
 5. (Page 13) *Funding*

a. (Page 13) 2002 HAVA and 2018 HAVA Election Security Funding

B. (Page 14) National Elections Organizations – National Association of Election Directors (NASED), National Association of Secretary of States (NASS), National Association of State Chief Information Officers (NASCIO), National Association of State Technology Directors (NASTD), National Institute of Standards and Technology (NIST), Election Center

1. (Page 14) *Providing Security Best Practices (NASED, NASS, NASCIO)*

C. (Page 15) State of Wisconsin Enterprise Level – Wisconsin Division of Enterprise Technology (DET), Wisconsin National Guard, State Law Enforcement

1. (Page 15) *Server Hosting and Management*

a. (Page 16) Firewalls

b. (Page 16) Server Patching

2. (Page 17) Phones

3. (Page 17) *Email*

a. (Page 18) Blocking and Defanging Malicious Emails

b. (Page 19) Inspection of Files and Analysis of Packets

4. (Page 20) *Monitoring and Alerts*

a. (Page 20) Monitor Threats

i. (Page 20) Analyze State Systems Activity to Identify Breach

ii. (Page 20) Alerts from FBI and DHS

5. (Page 21) *Desktop Support*

a. (Page 21) Infected Workstation Support

b. (Page 22) Desktop Imaging

c. (Page 22) Software Support

6. (Page 22) *Fusion Center- Planning*

a. (Page 23) Secret Security Clearance

7. (Page 23) *Provide Cyber Security Training*

a. (Page 23) Required Cyber Security Training Modules for State Users

b. (Page 24) Available Training for Local Users Not on State Network

8. (Page 24) *Provide 24-Hour Support Around Election Day*

D. (Page 24) State Elections Level - State of Wisconsin Elections Commission

1. (Page 24) *Development of Training*

a. (Page 25) Election Security Tabletop Exercises (TTX)

b. (Page 26) Security Training Videos and Webinars

c. (Page 26) Security Checklists

d. (Page 2) Other Training Resources

2. *(Page 27) Communications*
 - a. *(Page 27) Public Information Campaign*
 - b. *(Page 28) Secure Communications Portal*
 - c. *(Page 28) RAVE Communication with Local Elections Officials*
3. *(Page 28) WisVote*
 - a. *(Page 29) User Permissions and Distribution of Client Access Licenses*
 - b. *(Page 30) System User Policy*
 - c. *(Page 30) User Passwords*
 - i. *(Page 30) Multi-factor authentication*
 - ii. *(Page 31) Password Recovery Process*
 - d. *(Page 31) Management of System Reports and Information*
 - e. *(Page 32) Systems Testing*
 - i. *(Page 32) On-staff Security Personnel*
 - ii. *(Page 32) CompTIA Security Certified Staff*
 - iii. *(Page 32) Endpoint Testing*
 - f. *(Page 33) MyVote*
4. *(Page 34) Servers*
 - a. *(Page 34) Patching (In-house schedule vs. DET)*
 - b. *(Page 34) Encryption of Data at Rest and in Motion*
 - c. *(Page 34) Nightly Comparisons of Database Changes*
5. *(Page 35) Voting Equipment*
 - a. *(Page 35) State Testing and Certification*
 - b. *(Page 35) Audits*
6. *(Page 36) Election Night Reporting/Canvass*
 - a. *(Page 36) System Security and Training*
7. *(Page 37) Legal Infrastructure*
 - a. *(Page 38) Statutory References*
 - b. *(Page 38) Implementing Legislative Changes*
 - c. *(Page 36) Secret Clearance for Election Officials*
8. *(Page 39) Election Security Committees and Councils*
 - a. *(Page 39) Election Security Clerk Advisory Committee*
 - b. *(Page 40) Election Security Council*

E. (Page 40) County Level – County Clerk, County IT Departments, County Sheriff’s Office

1. *(Page 40) WisVote*
 - a. *(Page 41) Hardware & Software Requirements*
 - b. *(Page 41) Staff Security Measures*
 - c. *(Page 41) WisVote Provider/ Relier Relationship*
2. *(Page 41) Voting Equipment*
 - a. *(Page 41) Programing of Voting Equipment*
 - b. *(Page 42) Secure Storage of Equipment Between Elections*

3. *(Page 42) Election Night Reporting/Canvass*
 - a. *(Page 42) Posting Unofficial Results and Entering Results into Canvass System*

F. (Page 43) Municipal Level- *Municipal Clerks, Local Law Enforcement*

1. *(Page 43) WisVote*
 - a. *(Page 43) Hardware & Software Requirements*
 - b. *(Page 44) Staff Security Measures and Multi-Factor Authentication*
 - c. *(Page 45) Managing and Entering Voter Info for Municipality*

2. *(Page 45) Electronic Poll Books*
 - a. *(Page 45) Hardware & Software Requirements*
 - b. *(Page 46) Staff Security Measures*

3. *(Page 46) Voting Equipment*
 - a. *(Page 46) Initial Logic and Accuracy Testing of Voting Equipment Programming*
 - b. *(Page 46) Public Test of Voting Equipment*

G. (Page 47) Poll Workers and Other Local Users

1. *(Page 47) Voting Equipment*

2. *(Page 48) Electronic Poll Books*

3. *(Page 48) Polling Place Incidents and Disaster Response*

H. (Page 49) Public Level

1. *(Page 49) Voter Education and Preparation*

Section II: Election Security Incident Response and Communications

A. (Page 50) U.S. Government Level - Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), *U.S. Elections Assistance Commission (EAC)*, *Federal Voting Assistance Program (FVAP)*.

1. *(Page 50) Monitoring Threats and Alerting States*
2. *(Page 51) National Emergency Management*

B. (Page 51) National Elections Level – *National Association of Election Directors (NASED)*, *National Association of Secretary of States (NASS)*, *Coordinating Council*.

1. *(Page 51) Alerting States of Known Threats*

C. (Page 52) State of Wisconsin Enterprise Level – *WI Department of Enterprise Technology*, *Wisconsin National Guard and Emergency Management*

1. *(Page 52) Alerting Agency to Known Threats*
2. *(Page 52) Organization of Fusion Center*
3. *(Page 53) Wisconsin Emergency Management*
4. *(Page 53) State Server Isolation, Load Balance, and Recovery*

D. (Page 53) State Elections Level - *State of Wisconsin Elections Commission*

1. *(Page 53) Emergency Authority of WEC and Governor*
2. *(Page 54) Fusion Center (Incident Response)*
 - a. *(Page 54) Communication of Incident to Stakeholders*
 - b. *(Page 54) Provision of Support to Elections*
 - c. *(Page 54) Coordination with Wisconsin Emergency Management*
3. *(Page 54) WisVote Database Breach*
 - a. *(Page 54) Loss of Data Response Plan*
 - b. *(Page 55) Data Breach Response*
 - c. *(Page 55) Data Altered Response Plan*
4. *(Page 55) State Law Enforcement – Department of Justice*
5. *(Page 55) Internet Outage, MyVote Outage, WisVote Outage, or Server Event*
 - a. *(Page 55) Online Voter Registration*
 - b. *(Page 56) WisVote*
6. *(Page 56) Emergency Response Documents*
 - a. *(Page 56) Contingency Plan for Agency*
 - b. *(Page 57) Emergency/Disaster Contingency Plan for Local Election Officials*

E. (Page 57) County Level – County Clerk, County IT Departments, District Attorneys, County Law Enforcement

1. (Page 58) WisVote
2. (Page 58) Voting Equipment
3. (Page 59) Incident Response

F. (Page 59) Municipal Level- Municipal Clerks, local law enforcement

1. (Page 60) WisVote
2. (Page 60) Voting Equipment
3. (Page 61) Incident Response

G. (Page 61) Other User Levels- Poll worker responsibility, local law enforcement

1. (Page 62) Voting Equipment
2. (Page 62) Electronic Poll Books

H. (Page 63) Public Level- Voters, Voter Groups

1. (Page 63) Training, education, media

Election Security Report

Wisconsin Elections Commission

The Wisconsin Elections Commission has worked to examine all aspects of security in relation to Wisconsin's election administration technology and laws, and drafted a comprehensive report concerning the coordination between the WEC and various other election security partners. Wisconsin's election systems are secure thanks to the Wisconsin Elections Commission's strong partnerships with federal and state agencies, as well as with local election officials and the voters of Wisconsin. This report exists to detail the WEC's election security preparation and progress over the past two years, and steps WEC staff will pursue in the future to continue to keep Wisconsin's elections secure.

The report is broken into two sections:

- **Section I: Elections Security Preparation and Incident Prevention**

The Preparation section of the report is divided by level of government; each level is then further defined by roles and elections security considerations. For example, at the U.S. Government Level, the team is examining system monitoring activities and best practice guidance issued by agencies such as the U.S. Elections Assistance Commission (EAC) and the U.S. Department of Homeland Security (DHS). In the Municipal Level of the outline, WEC staff has analyzed what resources municipal clerks need to securely use technology such as the WisVote system, electronic poll books, and electronic voting equipment.

- **Section II: Election Security Incident Response and Communications**

The Response and Communications section of the report is also divided by level of government. The section includes short descriptions of the role that level of government plays in Wisconsin's elections, and includes mock election security incident situations and suggested responses and communication efforts. This section is meant to assist local election officials to create or update their existing election security contingency plans, and to see the importance of communicating any incidents to the proper authority.

For more information, please contact the Wisconsin Elections Commission at 1-866-VOTEWIS (1-866-868-3947), or at elections@wi.gov.

Section I: Election Security Preparation and Incident Prevention

A. U.S. Government Level

The State of Wisconsin Elections Commission (WEC) works closely with the Federal government to ensure compliance with federal law and to apply nationally recognized best practices to Wisconsin elections administration and election security initiatives. Specifically, the WEC coordinates election security efforts with the Department of Homeland Security (DHS), the U.S. Elections Assistance Commission (EAC), and other federal agencies.

The Elections Assistance Commission (EAC) is an independent agency of the United States government created by the Help America Vote Act of 2002 (HAVA). The Commission serves as a national clearinghouse for resources and information regarding election administration, including election security. The EAC is charged with developing guidance to meet HAVA requirements, adopting voluntary voting system guidelines, accrediting voting system test laboratories, and certifying voting equipment. The EAC also helps to coordinate election officials around the country so that they can share information and benefit from one another's experiences and processes.

The U.S. Department of Homeland Security (DHS) is responsible for safeguarding the country's infrastructure from physical and cyber threats that can affect national security, public safety, and economic prosperity. DHS works with election officials throughout the country to coordinate efforts to secure the elections process from both physical and cyber threats. DHS also coordinates with the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC), to provide services and information sharing that enhances the ability of government agencies to prevent and respond to cyber security events.

1. Certification of Voting Equipment (EAC)

One of the major responsibilities of the EAC is the certification of voting equipment. Vendors apply to the EAC to request certification of new systems and to request certification to new components of existing systems. The EAC's certification of voting equipment ensures that there is a consistent standard of reliability and security applied to all systems. More information on the EAC's process for certifying voting equipment can be found here:

<https://www.eac.gov/voting-equipment/system-certification-process/>

In 2005, the EAC adopted the first set of Voluntary Voting System Guidelines (VVSG), as mandated under HAVA. HAVA also requires that the EAC provide certification, decertification, and recertification of voting systems as well as the accreditation of testing laboratories. The EAC accredits independent test laboratories (voting system test laboratories or VSTLs) that evaluate voting systems and software against the VVSG to determine if the equipment provides all of the basic functionality, accessibility, and security capabilities required of voting systems. The test laboratory, based on its findings, provides a recommendation to the EAC.

The Commission's Certification Division, working through the Executive Director, makes the final determination whether to issue a certification. Once a decision has been made, the EAC posts the information on the Voting System Certification section of the EAC Web site. Therefore, an EAC certified voting system is one that has been tested by a federally accredited test laboratory and has successfully met the requirements of the VVSG.

The purpose of EAC's national voting system certification program is to independently verify that voting systems comply with the functional capabilities, accessibility, and security requirements necessary to ensure the integrity and reliability of voting system operation, as established in the VVSG.

2. Providing Security Best Practices (EAC and DHS)

a. EAC - Managing Election Technology Documents

Among the resources that the EAC has available for states to consider is its guidance for securing election equipment and systems. The EAC webpage that contains resources under this umbrella can be found here: <https://www.eac.gov/voting-equipment/managing-election-technology/>. Individual resources available through the EAC's "Managing Election Technology" webpage are outlined below in sections i-v.

i. Ten Things to Know About Selecting a Voting System

The EAC checklist "[Ten Things to Know About Selecting a Voting System](#)" is for local election officials who are considering the purchase of new voting equipment. The checklist reminds local election officials that they will need to consult their state's laws prior to making a purchase. It also encourages the decision maker to consider how much training will be needed for election inspectors who will be using the new equipment to ensure that they are familiar with security procedures. While the WEC is not involved in local election officials' voting equipment purchasing decisions, municipal and county clerks often request resources for consideration from the WEC staff. WEC will provide this EAC checklist to Wisconsin localities who are seeking resources as they consider any potential voting equipment purchase decisions.

ii. Ten Things to Know About Managing an Aging Voting System

Another checklist provided by the EAC to state and local elections officials is its "[Ten Things to Know About Managing an Aging Voting System](#)" checklist. This checklist provides tips for state and local jurisdictions to analyze their voting systems to ensure that the system still meets federal requirements and best practices. It also gives helpful tips on what to train poll workers to look for when preparing and operating voting systems to ensure that they are fully functional. The tips provided in this checklist are in addition to the rigorous testing and audit protocols mandated by state law.

For the State of Wisconsin, this checklist is a useful addition to the suggested poll worker training guidance and can be incorporated as a resource for clerks who are conducting poll worker training. The resource itself is intended for local jurisdictions who have direct interaction with their voting systems. While the general concepts listed on the checklist are already a part of the WEC poll worker training template, the format and reminders can be used to supplement current training materials.

iii. Considerations for Implementing Voting Systems with COTS Products

The EAC also provides a [checklist](#) for considering and implementing voting systems that utilize Commercial Off-the-Shelf products (COTS) such as laptops or tablets rather than proprietary vendor hardware. At this time, the WEC has not received any applications for COTS-based voting systems and is not aware of any COTS-based vendors. Should a COTS-based voting equipment vendor application be submitted to the WEC, staff would utilize the EAC checklist to ensure that the testing and approval protocol was designed to evaluate system security.

iv. Checklist- Securing Voter Registration Data

The U.S. EAC created the "Checklist for Securing Voter Registration Data" to provide election officials information and best practices to protect their voter registration data, and to provide assurance to members of the public that those security measures have been implemented.

Several components of the checklist have been implemented in Wisconsin including:

- Access control – only authorized users with credentials and a multi-factor authentication tool can access WisVote.
- Auditability – WisVote includes a full audit trail including who made changes, on what date, and what the values were before and after the change.
- Data Backups – the WisVote database is backed-up nightly in two physically separate locations.
- Firewalls – the Wisconsin Department of Administration's Division of Enterprise Technology (DET) maintains all firewalls for the Elections Commission, including the firewalls used to protect WisVote.

- System Interconnection – WisVote is maintained on DET servers and uses a separate Active Directory Domain Controller to help isolate it from other systems. WisVote is connected to related elections applications but these connections are secured in a variety of ways to prevent unauthorized access.
- Documentation – The BadgerVoters website maintains logs of voter data purchased by the public as well as information regarding who purchased the data and when. WisVote IT staff maintains change management logs to document any updates to the system design, and all activities within WisVote that impact voter data are logged, including what user took those actions.

There are additional best practices included in the checklist that the WEC is continuing to implement including the establishment of additional criteria in WisVote to trigger unusual activity notifications such as multiple log-in attempts, unusual traffic, or large amounts of data uploads and exports.

v. Checklist - Securing Election Night Reporting Systems

In Wisconsin, counties are required to post all returns, by ward or reporting unit on an Internet site. Many jurisdictions use a separate Election Night Reporting (ENR) system to display unofficial election night results to the public through a web-based application. The [U.S. E.A.C. Checklist for Securing Election Night Reporting Systems](#) provides a baseline for jurisdictions to assess the security protocol surrounding their Election Night Reporting system.

Whether a jurisdiction reports election night results using an ENR or some other method, the checklist includes items that are useful for all jurisdictions. Each county should review the checklist for the points relevant to the method that is used for election night reporting. All counties should proof the data being posted on election night and validate that results shown on their website match the results reported by municipalities and have a backup plan should their website become unavailable. They should also ensure that they have received results from all reporting units and post a disclaimer along with the results if data from any reporting units is missing.

All jurisdictions should include election night results in their continuity of operations and risk management plans. Election night results are unofficial, but the public does not necessarily perceive them as unofficial. Therefore, providing assurance to the public that the election night reporting systems (whether ENR software or a home-built spreadsheet) are accurate and protected is of the utmost importance to every election official.

b. DHS Resources and Best Practices

Another source for information on Election security is the Department of Homeland Security. DHS provides guidance specific to voter registration data as well as information on overall cyber security best practices. DHS resources are discussed below in sections i-iii.

i. Security Tips for Securing Voter Registration Data

DHS has resources available for states to assist in securing voter registration data. DHS recognizes that voter registration databases are rich and attractive targets for computer intrusions. The keys to good cyber security are awareness and constant vigilance. There are many threats DHS articulates that can put voter data at risk, such as phishing attempts to get credentials from users, injection attacks, XSS vulnerabilities, denial of service attacks, or ransomware. The US-Cert program which is described in Section 3 below has extensive publications regarding how to handle many of these threats. The WEC staff has completed extensive review of the US Cert publications, and recommendations related to US Cert are found elsewhere in this report.

In addition to the US Cert documentation, DHS makes several basic recommendations that can prevent as many as 85 percent of targeted cyber-attacks. Many of these recommendations are already in place in Wisconsin or are being implemented such as:

- Patching of applications and operating systems
- Application whitelisting through DET
- Restrict administrative privileges
- Input validation
- Firewalls

DHS has also created a list of questions that election authorities should consider assessing their ongoing security preparations. WEC has performed this recommended exercise and has implemented suggested security patches to continue to prevent targeted cyber-attacks.

Lastly, DHS gives critical recommendations for how to respond if unauthorized access to voter registration data occurs. First, an event such as this should trigger our security incident response plan and business continuity plan. It is important to maintain essential functions for the agency while allowing time for IT staff to isolate and remove the threat. Second, it is important to contact DHS and/or law enforcement immediately. The WEC has created and solidified a continuity and communications plan to quickly control, resolve, and communicate a security incident.

ii. Best Practices for Continuity of Operations (Handling Destructive Malware)

Malware is an umbrella term used to describe a variety of intrusive software programs such as computer viruses, trojan horses, ransomware, spyware, and other programs that pose a threat to user applications and hardware devices. DHS has provided a best practice document on how to protect systems, including elections systems, from malware activity.

The WEC and DET are following many of the recommendations found in this document. The WEC election management systems are largely secured behind layers of security within the DET data center. A next-generation firewall system is well organized, monitored, and regularly updated. Minimum ports and protocols are configured for host-to-server and host-to-host connectivity. Servers and applications are categorized into tiers with individual plans in place.

Also, the WEC and DET have backup systems in place which are monitored daily. Service accounts are tightly controlled and limited to specific functions. Systems are monitored for utilization and anomalous traffic or patterns. Vendor patching is regularly scheduled and offset between all system environments allowing for thorough testing opportunities.

In addition, the WEC has the recommended COOP recovery planning in place, as well as documentation of critical asset dependencies, contacts, and organizational information.

iii. Ransomware: What It Is and What to Do about It

Ransomware is a type of malicious software that threatens to publish the victim's data or block the victims' access to required information until ransom is paid in the form of information or data from the victim's computer. DHS has published guidance on how to protect systems, including election systems, from ransomware attacks.

As recommended in the DHS guidance on ransomware, the WEC has the following systems in place to protect Wisconsin's election management systems:

- Daily offsite backups are maintained and regularly verified. Access to backup data is segregated from critical data and applications to prevent ransomware from spreading to backup data.
- Backup systems are in place so that critical data and applications can be restored quickly in the event of an outage.
- COOP recovery planning is in place, documenting critical asset dependencies, contact and organizational information.
- A centralized patch management system is in place and all systems are patched regularly.
- Active administrative accounts are limited, and user roles are restricted to necessary access.

WEC internal operations have the advantage of being located on the state supported LAN/WAN with a centralized file share. Inbound and outbound email traffic is filtered through a security appliance, which strips and defangs suspicious emails, links or attachments. A web content filtering gateway is also in place blocking risky or known malicious web sites and IP addresses. Macro scripts are stripped from incoming MS Office attachments. Staff has also participated in several cyber security awareness training programs over the past few years. Protocols are in place to identify and manage the infection of a device.

3. Training for State and Local Governments

Agencies within the U.S. Federal Government and associated agencies provide learning tools and opportunities for state and local election officials to consider. Training resources available through the federal government are listed below in sections a and b.

a. Training Resources

i. FEDVTE (DHS)

This recommended training resource was produced by the federal government and offers courses principally for more technical users, but some classes have more general applicability. The training curriculum contains extremely detailed and advanced technical training. Some WEC staff have currently enrolled in FEDVTE training curriculum including the following courses:

- 101 Critical Infrastructure Protection
- Cyber Security Overview for Managers
- Cyber Risk Management for Managers
- Static code analysis and settings evaluation
- DoD IA Boot Camp

ii. US CERT(DHS)

The Computer Emergency Readiness Team website provides an extremely comprehensive set of information, including links to most of the resources in this document. WEC staff is currently subscribed to and analyzing the following communications:

- **Newsletters** – These include alerts on newly-discovered vulnerabilities and exploits, general tips and current events.
- **Publications** - There are dozens of publications on this website covering a wide variety of cyber security topics from creating secure passwords to technical details on specific attacks.

- **C³ Resources for State, Local, Tribal and Territorial Governments** - Useful information to incorporate into WEC security curriculum for local election officials.

iii. OnGuardOnline (Federal Trade Commission)

OnGuardOnline is a training resource more focused on families with children and primarily offers information that is of limited use to municipal clerks or state elections system users. The non-child based information overlaps with the standard web security information provided by DHS. Aspects of this training and links to helpful videos have been included in the WEC-created Security Awareness webinar series for Wisconsin's local election officials.

iv. Stay Safe Online (National Cyber Security Alliance)

Stay Safe Online appears to be the parent cyber security program and references to Stop Think Connect for many points. Stay Safe Online is still useful as a resource because it includes more in-depth information and definitions over what can be found on Stop Think Connect. Also, Stay Safe Online includes additional resources for businesses, reporting cyber-attacks (of limited use to our needs), and a section dealing with mobile devices. Aspects of this training and links to helpful videos have been included in the WEC-created Security Awareness webinar series for Wisconsin's local election officials

v. Stop. Think. Connect. (National Cyber Security Alliance)

Stop. Think. Connect. is an awareness campaign associated with the Stay Safe Online program. As a separate awareness campaign, the website includes a Resources section with multiple tip sheets, radio and Internet PSAs, and posters/memes for use by the public. For this training to be useful, local election officials would need to have previous knowledge of, and follow, a base level of cyber security. While some aspects of this training resource have been incorporated into the WEC election security curriculum for local election officials, the resource continually must be framed appropriately for it to be effective in the context of elections.

b. EAC in-Person Trainings for Local Election Officials

Through communications with state election officials, the EAC has offered to send an EAC Commissioner and/or staff member to local election official conferences or events to discuss election security. Some states with a centralized election administration structure, where all county clerks meet at a yearly conference, have invited the EAC to speak at their events. Those states report the presentation as being well received by local election officials.

In September 2018, representatives from the EAC attended a meeting of the Wisconsin County Clerks Association, as well as an official Wisconsin Elections Commission meeting with members of the Commission attending. The WEC is pursuing additional opportunities for including an EAC speaker at future Wisconsin County Clerks Association, Wisconsin Municipal Clerks

Association (divided into nine districts), and Wisconsin Towns Association meetings. However, unlike other states, there is no single event where all of Wisconsin's 1,900+ municipal and county clerks gather in one centralized location for an event.

i. DHS Tabletop Exercises

In October of 2018 and July of 2019, the Department of Homeland Security conducted an election security tabletop exercise in Madison, Wisconsin. The exercise included federal, state, and local partners. The exercise brought together the many different partners who play a role in the election process to work with sample election security incidents that can occur in the time before and after Election Day and find sample resolutions. The exercise also allows for different election partners to identify and connect with potential resources that can help resolve any potential incidents.

The WEC continues to work with the Department of Homeland Security to schedule future DHS-led TTX events in Wisconsin to further involve local election officials and other state and federal partners ahead of the 2020 elections.

ii. DHS Poster Guide for Local Elections Officials

The Department of Homeland Security has created customized election security posters for local elections officials to use in their communities. These posters contain location-specific information concerning safeguards and resiliency measures already in place, threat mitigation efforts, and initiatives that the localities are undertaking ahead of the 2020 election cycle.

Due to Wisconsin's large number of local election officials, DHS was not able to create and distribute a poster for each municipality and county in the state. WEC staff worked with DHS to create a brochure that is more applicable to Wisconsin's unique election system.

The brochure contains a checklist on how to best prepare and prevent a security incident by utilizing federal and state resources available to all clerks, how to safeguard an election system, how to determine if there is a cyber incident or unusual activity at a polling place, some sample guides on how to respond to a variety of security incidents, and additional resources and templates clerks can use. The brochures will be available for clerks before the 2020 election cycle.

4. Critical Infrastructure Designation & Monitoring Activity (DHS and FBI)

a. Defining the Designation for Wisconsin

The Department of Homeland Security designated elections systems as critical infrastructure in 2017. According to the DHS website, a critical infrastructure designation is given to “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”

For state election officials, the designation as critical infrastructure means that state and local elections agencies have more access to additional resources through DHS and other federal agencies. It also means that there is a heightened awareness and priority given to elections agencies in terms of providing such services at times of critical need.

b. Coordinating Council

When a sector is designated as critical infrastructure, federal law requires that a coordinating council, specific to that sector, be created. In 2017, the Government Sector Coordinating Council (Council) was created by DHS to facilitate effective communication and coordination of critical infrastructure between the federal, state, and local governments. The goal of the Council is to inform the work of DHS in the elections field and to help establish clear communication protocols between DHS and the appropriate state election officials.

In the summer of 2017, the membership of the Council was established, and the Council has since met to establish a charter and begin discussions. While the State of Wisconsin is not currently represented on the Council, WEC leadership continually communicates with the EAC, DHS, and the National Association of Election Directors (NASED) which are represented on the Council to convey the needs and concerns of Wisconsin election officials.

c. Providing Regular Scans

DHS provides cyber monitoring, scanning, and evaluation tools to elections agencies. Among these resources is the National Cybersecurity Assessment & Technical Services (NCATS). The NCATS leverage the best cyber security assessment methodologies, commercial best practices and integration of threat intelligence that enable cyber security stakeholders with decision making/risk management guidance and recommendations. NCATS provides an objective third-party perspective on the current cyber security posture of the stakeholder’s networks. NCATS security services are available at no cost to stakeholders and can range from one day to two weeks depending on the security services required.

The WEC has utilized the DHS NCATS service since 2016 and has an NCATS scan performed on agency IT applications weekly. WEC staff receives a report from the NCATS scans which is then analyzed by WEC staff to identify issues and recommendations. Any recommendations or patches are then deployed on agency applications or relayed to DET which deploys server-side fixes.

DHS has other scanning and monitoring resources that WEC is exploring in conjunction with DET. Other resources include physical site assessments for municipalities, risk vulnerability penetration testing and cyber infrastructure surveys.

d. Risk Vulnerability Assessment (DHS)

To identify and limit vulnerabilities in election systems and applications, DHS provides a Risk Vulnerability Assessment (RVA). The RVA is a penetration test that is focused on an election agency's applications including WisVote and MyVote. A penetration test, or pen test, is a simulated attack on a computer system that is authorized by the owner of the system to identify security vulnerabilities that could lead to a malicious actor gaining unauthorized access to a system's functionalities or data.

The DHS RVA is an intensive review of elections systems that mimics potential hacking scenarios like social engineering, remote system access, database scanning, and manipulation and email phishing campaigns. The RVA is conducted over a two-week span. During the second week, DHS staff will be onsite at the WEC. Both during the assessment and following its conclusion, DHS staff will provide WEC with a report of security options and suggestions for improvement. There is no cost to the WEC for the RVA, but the WEC will need to dedicate significant staff time and agency resources to the RVA for at least two weeks. An RVA of the WEC's applications was completed in September 2018, and future RVAs are planned to occur on a regular basis.

e. EAC Resources

The EAC provides resources to state and local election officials to help them understand the DHS Critical Infrastructure designation. WEC staff members have analyzed the following resources to gain a better understanding of what the designation means for Wisconsin elections.

i. Elections Critical Infrastructure Hub and Glossary

The EAC website includes a [hub](#) specifically for Critical Infrastructure Designation (CID) materials. Among the materials is a glossary of CID terms that WEC staff uses when

communicating CID information to election partners including the Elections Commission staff, local elections officials, and the media.

ii. EAC “CI Scoop” Blog

The EAC also has a [blog](#) specific to the CID that provides analysis of timely issues related to the designation. The blog is a good resource for WEC staff who are involved in elections security to stay up to date with any changes or developments related to the designation. Much of the information contained in the blog is also disseminated to state election officials through other national groups that work with the Coordinating Council. WEC staff will continue to monitor the blog for new information that relates to elections in Wisconsin.

5. Funding

a. 2002 HAVA and 2018 HAVA Election Security Funding

The WEC maintains a balance of federal grant funds that were appropriated in 2002 through the federal Help America Vote Act (HAVA). These funds can be used to support most agency elections administrations functions including the development, maintenance of the statewide voter registration system, WisVote. Currently, the WEC uses HAVA funds to support the agency’s core functionalities, including providing training to local election officials, maintenance of WisVote, and the funding of staff positions. The WEC expects to deplete its 2002 HAVA funds in 2019. Currently, the remaining balance of funds are reserved for core election administration through 2019.

In March 2018, the WEC received a \$6,978,318 grant award to improve the administration of elections for Federal office, which includes technology enhancements and elections security improvements to its systems, equipment, and processes used in federal elections. Currently, the WEC has used funding to hire six federally funded positions focusing on election security, implement multifactor authentication programs for the WisVote system, update the WisVote Access Policy which includes the completion of cyber security-focused electronic training modules, and the creation and roll out of a robust election security tabletop exercise (TTX) program for local election officials. The WEC plans on using parts of the 2018 HAVA grant funds for future election cycles to ensure that necessary security updates can be implemented in the coming years.

B. National Elections Organizations

There are several national organizations that aim to coordinate professionals from across the country on important topics related to elections. The National Association of State Election Directors (NASED) is an organization comprised of the chief election official from each state. WEC Interim Administrator Meagan Wolfe was selected as the Midwest Regional Representative of NASED at its 2019 Winter Conference. As Midwest Regional Representative, Administrator Wolfe will represent the interests of the other midwestern state election directors on the NASED Board. NASED coordinates conferences, events, and communications to its members on important elections information including elections security. NASED has played a role in working with DHS and other organizations to appoint members to the Government Sector Coordinating Council. NASED coordinates information sharing among state election directors so that all states can benefit from best practices and lessons learned.

Organizations such as the National Association of Secretaries of State (NASS) and the National Association of State Chief Information Officers (NASCIO) are also involved in elections related matters. In many states, the Secretary of State is the chief election official and is very involved in elections security. Because the Wisconsin Secretary of State is not involved in elections administration, the WEC has reached an agreement with NASS to subscribe to its election related services and resources for a reduced membership rate. NASCIO is also an important election security partner, as many states, including Wisconsin, rely heavily on the office of the state Chief Information Officer to provide front line defense for election systems and servers.

1. Providing Security Best Practices (NASED, NASS, NASCIO)

WEC staff receives regular communications from NASED, NASS, and NASCIO. WEC staff analyzes these communications for information that is relevant to Wisconsin elections. For example, NASED will pose elections related surveys to its members and, as a result, all states are able to learn from the results. NASED also hosts events and conferences which are an excellent opportunity for election officials across the country to learn from one another and other partner organizations to and coordinate on best practices. When NASS holds conferences or events that cover election related topics, WEC staff receives an invitation to attend. WEC staff attended NASS “Tech Talk” events in 2018 to coordinate with its membership to stay up to date on elections security and technology. WEC staff will continue to monitor these organizations for information and resources that are applicable to elections in Wisconsin.

C. State of Wisconsin Enterprise Level

The Wisconsin Elections Commission (WEC) is an agency within the State of Wisconsin government. While the WEC is an independent state agency, it utilizes enterprise level technology services available through the State of Wisconsin Division of Enterprise Technology (DET). DET, housed within the Wisconsin Department of Administration (DOA), provides many services to the WEC including server hosting and management, phone and email hosting, and desktop imaging and support. The WEC also has other security partners at the state enterprise level including Division of Emergency Management, the National Guard and state and local law enforcement. In preparing for an election related security disaster or emergency management event, the National Guard and State level law enforcement have been able to provide resources and guidance. The WEC communicates regularly with state level enterprise partners and has regular meetings with such agencies to better understand and coordinate their roles in elections security prevention and response.

1. Server Hosting and Server Management

DET hosts the servers that power the State of Wisconsin's voter registration database, known as WisVote, as well as related applications such as the MyVote Wisconsin website. While the WEC staff builds, maintains, and secures the applications themselves, there is a great benefit to having the servers hosted through DET. The DET server structure is arranged so that there is one single point of control of the state enterprise server system. DET deploys sophisticated firewalls and monitoring techniques at the single point of entry to ward off malicious and extraneous activity. Visibility and traffic monitoring tools deployed by DET and a sensor supplied by the Multi State - Information and Analysis Center (MS-ISAC) in conjunction with DHS are used at the single point of control to allow DET, as well as the MS-ISAC security operations center, to evaluate each contact with the state enterprise server system.

DET further protects state servers by dividing the server environment into zones. Each zone is then further monitored by a diverse set of cyber tools to analyze server activity. Adding to the complex and layered server security set up, server zones are assigned unique firewalls to further prevent attacks or extraneous activity. The additional zones and protections ensure that if a malicious actor is able to breach the single point of control, there would be other security measures in place to prevent attacks on any specific zone or server. The division of servers also allows applications to be isolated and protected according to the specific needs of the applications and to allow redundancy of system monitoring by protecting various zones with different monitoring tools than are used at the single point of control.

a. Firewalls

DET uses firewalls to protect the state enterprise servers at many points throughout the server topography. In addition to using firewalls at multiple points throughout the system structure, DET also uses a variety of firewalls. Having a variety of firewalls increases the amount of information available to prevent an attack. Each firewall sources its information differently, such as by monitoring activity across the DHS network or by sourcing information from corporate partners. Firewalls operate using a dynamic base of information to archive and prevent attacks, using information sharing throughout the cyber security world. The more sources that can be used to create the database of known and suspicious actors and methodologies for blocking them, the more comprehensive the firewall protection.

New information is being added to the DET firewall database all the time. The information comes from national, military, corporate and state sources, including from state employees. If an agency, state employee or state customer becomes aware of a potential threat they are instructed to report the threat to DET. When reporting a potential incident or threat to DET, the user is asked to provide information such as server information, IP addresses, and server ports involved in the incident. DET then places a hold on activity by the potentially threatening IP address or actor while it investigates the activity. If the activity is identified as potentially malicious, DET then adds the information to the firewall database of blocked users and deploys other methods to block further contact with the suspicious actor.

b. Server Patching

Another service that DET offers to protect state servers is patching. Patching is a process through which software is deployed to update a computer program, operating system, or server to support data, fix a known bug, or make an improvement. Patching also includes deploying fixes to remedy security vulnerabilities. Like firewalls, servers and programs need to be kept up to date with the most current information, and patches are used to add that current information to the server or program. DET also provides patching auditing of servers which is a service that compares programs against a list of patches to ensure compliance.

DET deploys patches as part of a regular schedule. The schedule is developed with the business needs of agencies across the state enterprise system in mind. If a patch is deployed on a server or zone that supports one agency, there could be an impact on other agencies who share the server space. Patches need to be tested across the entire server structure to determine if the patch may cause unintended consequences on other areas of the server environment. Sometimes when a patch is deployed, the servers or server zones need to be restarted, causing short outages. Because of this, the DET patching schedule includes change freezes where only

emergency patches can be implemented to avoid outages during critical business operations. In coordination with WEC, DET has implemented a change freeze protocol during important times in the election cycle. Patches that are not critical cannot be implemented on any DET server in the week prior to a major election. This ensures that there are no server outages during critical elections periods unless a special exemption is granted by the Chief Information Officer.

2. Phones

DET provides phone services for state enterprise users. Currently, DET is in the process of transferring phone services to Voice Over Internet Protocol (VOIP) which connects phone and email services through a unified communications platform. A unified platform allows state users to connect via phone from anywhere using their Windows computer or mobile device. The platform also allows DET to integrate phone services with other software applications, which provides more consistency with maintaining patches and overall security.

The WEC switched from traditional phone service to VOIP as part of a statewide roll-out in early 2019. This will allow staff time to learn the new system and transfer to the new integrated platform in time for the uptick in calls for the 2020 election cycle. The integrated VOIP platform will allow the WEC additional opportunities to track calls and voicemails which can also be used to monitor and analyze call activity to identify trends that may need additional attention.

3. Email

Enterprise e-mail services through DET provide state agencies with a centrally managed, enterprise-wide messaging system. In addition to email and calendar functions, the DET enterprise email system provides anti-spam and anti-virus protection, file-sharing services, outbound faxing, the ability to send encrypted email, email archiving, backup services, and helpdesk support. DET hosts email services for 30,000 state users with a resilient configuration in multiple locations. [The Email Service Roles and Responsibilities \(R&R\)](#) document delineates how specific responsibilities are divided between DET and agencies.

DET is the first and primary layer for security and support for all state user email accounts, including the WEC. To protect state user emails, DET maintains multiple copies of each email database on multiple servers. The many layers to the state email storage architecture ensures that information is not lost and can be recovered. It also allows DET to resolve known issues without outages by directing state email systems to a backup server while testing or patches are implemented in the main environment.

DET also uses virtual separation to create security boundaries between agencies. Agencies are separated by rights, permissions and within the domain structures provided for agencies. Agency account attributes, like the marker that indicates elections applications and email accounts, are critical components of the email security structure because they ensure that only the users with the correct permissions can access information associated with an agency. All state user emails are secured and stored using the highest level of security required. For example, some agencies are subject to strict requirements, like HIPPA laws, because of the nature of their work. Therefore, the WEC and other agencies also benefit from these high standards being applied to all state enterprise email storage, security, and access permissions.

In addition to the enterprise wide hosting, storage, and security that DET provides for state email users, it also offers customized solutions that agencies can opt to use based on their needs. WEC continues to work with DET to explore additional options for using email services. Some of the options include digital signatures which could help to identify emails sent from elections employees as official so that clerks and elections partners can differentiate those communications from spam or phishing attempts. DET also offers other services such as routing outgoing emails through a secure portal, much like communications that are received from a banking institution. WEC and DET are exploring this service for sending security related messages to local election officials. This service would also offer additional email encryption options beyond the in-network encryption services that DET automatically applies to hosted accounts.

a. Blocking and Defanging Malicious Emails

DET provides the first line of defense against malicious emails for affiliated state agencies including the WEC. Using several criteria, including the digital reputation of the sender and number of transactions from the sender, DET identifies and then quarantines suspicious incoming and outgoing email messages so that malicious emails are not delivered to their intended target. There is a complex scoring system used to determine which emails DET should block and which emails should be sent to their intended recipient.

DET identifies and blocks a high volume of malicious or extraneous emails that are never received by state users. Monthly, DET blocks 90-95% of emails that are sent to state users. In one month, DET successfully blocked 62.4 million email messages from being received by state users. There is a very low instance of “false positives” in the DET blocking system, meaning very few legitimate emails are mistakenly identified as spam.

DET also “defangs” emails to remove potentially problematic links before sending to the recipient. Defanging is a process of removing or re-writing links within an email so that the

recipient cannot be directly routed to a malicious website through the URL in the emails. If an email passes DET's initial spam check, it is then scanned for links. The defanging process DET utilizes rates the reliability of links embedded in emails. If the link in the email is known to be legitimate, then the email is sent without any changes. If the link receives a less reliable rating, then the URL in the email is routed through a proxy server to re-write the URL before it is sent. If the link receives a low score, then the link is deactivated before the email is sent to the user.

There are many layers of information that DET employs to determine what emails should be blocked. Like any other security measure, such as firewalls, the list of SPAM email actors and tactics changes daily. DET works with other government agencies and vendors to keep the list of SPAM email actors up to date. An important part of keeping this list up to date is through receiving information from state email users. If a state email user receives a suspicious email, they are instructed to send and report the email to the DET helpdesk, which will investigate and then add the email to the spam list if appropriate.

b. Inspection of Files and Analysis of Packets

Another service that DET offers to agencies is what is known as packet analysis. Packet analysis is done through a program or a piece of hardware that can intercept and log traffic directed at a network or a specific part of a network. A packet is a group of data transmitted over a digital network. As the data is transmitted to the network, using any number of digital media, DET can anticipate the transmission and capture it for analysis before it reaches the server framework. DET can then analyze the packet and, if needed, decode the packet's data, showing the values of each field in the packet. Based on this analysis, DET can then deny the packet access to the state system or determine that it is legitimate and allow the packet to proceed to the next level of the security framework, such as a firewall, for additional analysis.

The file inspection and packet analysis services that DET provides to the WEC and state users have many layers. For the WEC, this means that malicious or extraneous data packets aimed at our systems are intercepted and analyzed before they ever reach the internal server security or firewalls. Every day DET intercepts and blocks numerous threats across the state enterprise using this structure.

4. Monitoring and Alerts

a. Monitors Threats

DET monitors threats to the state server structure and to WEC applications using a variety of internal and external information sources. Internal sources of information, like firewalls, activity logs, and hardware and software alerts and sensors are described in the DET server structure above. DET also monitors third party sources for threats and alerts. Many of the sources of third-party information comes from DHS and other federal government sources. DET also subscribes to commercial threat identification services that are renewed annually. DET also partners with the Wisconsin Department of Justice's Wisconsin Statewide Intelligence Center (WSIC) for sharing intelligence information with other states.

i. Analyze State Systems Activity to Identify Breach

Once DET receives an alert or notification of suspicious cyber activity, the activity and associated IP addresses are added to the database housed on system security devices. DET also deploys any suggested patches to seal vulnerabilities and prevent future contact with the offending cyber actor. The information of the suspicious cyber actor is also added to the blocked list on DET firewalls while DET continues to investigate.

DET also analyzes logs of previous activity across the server system to see if the malicious actor has had any previous contact with the State of Wisconsin IT Enterprise. If there is a log of previous activity, DET can then trace the activity throughout the server structure to determine if there was any impact on state systems. If an incident is identified, DET will notify the owner of that system to identify the scope of the problem and to implement a solution.

ii. Alerts from FBI and DHS

DET partners with the FBI, DHS, U.S. Department of Justice, the National Guard and other federal cyber security agencies through the Wisconsin Fusion Center. More information about the Wisconsin Fusion Center is detailed below in section 6. DET and WEC also have direct communication channels with DHS and have been assigned local and regional liaisons who provide security information.

Through its Cyber Security Division, DHS also works closely with the Center for Internet Security (CIS). The CIS is a non-profit organization that has created the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC), which partners with state governments and federal agencies about potential cyber security threats. The MS-ISAC and EI-ISAC receives cyber security information, alerts, and intelligence from across the country and coordinates that information so that all states can benefit. DET and WEC regularly receive information and alerts from DHS through the MS-ISAC

and the EI-ISAC. These alerts typically contain a recap of an incident that has occurred in other states and includes patches and tips so that states which have not been attached can proactively protect their systems.

Additionally, DHS utilizes sensors to monitor federal cyber networks to identify threats and shares that information with states via state fusion centers and the MS-ISAC. This intelligence information is used to protect state systems, including WisVote. The MS-ISAC provides sensors similar to DHS to state technology offices and monitors them around the clock. DET utilizes this service from the MS-ISAC at the main point of control of the state network to protect the IT infrastructure of WEC and other state agencies.

If DET receives federal cyber security information relevant to elections, that information is shared with WEC. If WEC receives federal cyber security information relevant to elections or any other state system, that information is shared with DET. Often both WEC and DET receive the same alerts and notifications from federal sources. DET and the WEC have partnered to create a communication chain to ensure that cyber security information is shared between both agencies.

5. Desktop Support

DET provides desktop support to agencies on the state network. These services include recommendations and procurement services for hardware, configuration, and imaging of new devices, software deployment and management, and operating system and software patching. These core services ensure consistency and security across the state network. DET's Desktop Roles and Responsibilities document outlines the services DET provides and what responsibilities agencies like the WEC have to maintain their desktops in a secure manner. The document can be found here:

<https://det.wi.gov/Pages/AgencyManagedApplicationService.aspx>

a. Infected Workstation Support

As part of the desktop support that DET provides to WEC and other agencies, it monitors traffic on the state network through a central server that intercepts traffic from each desktop. From here DET can determine if there is any unusual activity occurring on state desktops that might signal the desktop is infected with malware like adware, ransomware, or a virus. If unusual activity is flagged, DET will notify the IT staff at the agency registered to the PC to investigate. DET will then work with the agency to contain and correct the infection. DET maintains standard images for workstations so that in the event of infection the entire computer can be reimaged and returned to use very quickly. Most attacks are blocked by DET firewalls and other security measures before they reach and infect a state user's computer. Having this monitoring

in place ensures that WEC agency hardware remains free of viruses and other malware that could impact elections systems.

b. Desktop Imaging

Desktop disk imaging is another important tool that DET provides to agencies like the WEC. Desktop imaging is a computer file containing a computer's core systems including operating system, software and network structure for the device. DET first sets up the target environment conventionally, including installing end-user software as well as hardening the system according to industry best practices such as the Center for Internet Security's Controls. This initial set up also includes provisioning the device with DET's Enterprise security controls. DET then creates an image file from that machine and downloads it to all devices for a specific agency. The WEC benefits from utilizing DET's imaging process because it ensures that all agency hardware is configured in a secure and a consistent way. By keeping all work data on shared drives and utilizing centrally managed desktop applications, this process also ensures that in the event of an infection, a workstation can be quickly wiped and reimaged with minimal disruption to business processes.

c. Software Support

DET also provides software support to WEC. DET purchases customized software licenses at the enterprise level for agencies to use. This means that DET can analyze software to ensure that it is secure and that all terms and agreements comply with state standards before agencies are able to purchase or download the program. DET can also track which state users are using DET supported software to ensure that those users receive necessary software patches and that the software is kept up to date. While the WEC and other agencies need to purchase the software license from DET, the agency is receiving additional protections and guarantees that it would not receive if the agency were to purchase software independently.

6. Fusion Center- Planning

DET is a member of the Wisconsin Statewide Intelligence Center, one of Wisconsin's two Fusion Centers. The Fusion Centers are collaborative organizations that include state and federal agencies with the goal of sharing resources, expertise and information to detect, prevent, and respond to criminal activity, including cyber activity. The Wisconsin Statewide Intelligence Center is managed by the Wisconsin Department of Justice and includes members from DHS, the FBI, law enforcement, military services and critical state agencies.

DET staff attend weekly Fusion Center briefings on security concerns from around the state, nation, and world. The Fusion Center briefings provide government security partners a

classified space to share information and find solutions. DET is able to make state IT systems and servers more secure by utilizing intelligence information and IT resources from other security partners at the Fusion Center. Election security is sometimes discussed at Fusion Center meetings. The WEC is not directly a member of the Fusion Center but does participate in elections-related Fusion Center initiatives and is in regular contact with Fusion Center staff. Overall, WEC staff believe that the state election systems benefit from its efforts through DET's involvement.

a. Secret Security Clearance

DET has staff members who have Secret Security Clearance through the U.S. Department of State. Secret Security Clearance is a status granted to individuals to permit them access to classified government or military information after completion of a thorough background check. The DET staff members with Secret Security Clearance can communicate with others holding such clearance at agencies such as DHS and the FBI. DET can then work with other classified security personnel to formulate a solution to a classified problem. The action that is needed to remedy the issue can then be shared with unclassified staff who can deploy the fix.

Currently, the WEC has staff members that have Secret Security Clearance as part of the Critical Infrastructure designation. This designation allows for WEC staff to quickly obtain information from our federal partners concerning election security and implement suggested security measures. The WEC staff members with Secret Security Clearance coordinate efforts with the DET staff with Secret Security Clearance to prevent and respond to election related cyber-attacks based on classified information.

7. Provide Cyber Security Training

a. Required Cyber Security Training Modules for State Users

DET prescribes cyber security training that is required for all state enterprise users including WEC staff. DET requires all state system users to complete a curriculum of interactive web-based tutorials that focus on common cyber security threats like password security, phishing and spear phishing scams, identity theft and more. Training completion is tracked in the Enterprise Learning Management system to ensure all employees have completed the training. All WEC staff are required to complete the cyber security curriculum through DET. This mandatory training has been a valuable tool for WEC staff to understand the general concepts surrounding internet and cyber security.

b. Available Training for Local Users Not on State Network

The interactive training tutorials available to state enterprise users, like the WEC staff, are not available for distribution to local election officials. DET subscribes to the web-based security service at a cost and the subscription is only available to employees within the State of Wisconsin enterprise.

While DET does not have a cyber security curriculum for the WEC to distribute to local election officials, the WEC has created its own web-based tutorials for municipal clerks that is available on the WisVote Learning Center website. More about the training plan for local election officials is outlined in Section D of this report.

8. Provide 24-Hour Support Around Election Day

The Department of Military Affairs Division of Emergency Management has granted access to the WEC to utilize its 24-hour emergency communication hotline in the days around Election Day. This emergency hotline allows for local elections officials to quickly contact authorities if they suspect an election security incident has occurred outside of the WEC regularly scheduled office hours. WEM staff has coordinated the WEC to quickly relay any reported incidents to the appropriate WEC staff. The WEC published a one-page quick reference reporting guide for local elections officials ahead of the 2018 General Election and plans to do so for future elections.

D. State Elections Level

In the State of Wisconsin, the Elections Commission is charged with the oversight and administration of elections for the State of Wisconsin. The WEC is required to provide elections administration training, materials, guidance and support to Wisconsin's 1,852 municipal clerks and 72 county clerks. This includes providing election security training, information, and resources to Wisconsin's local elections partners.

1. Development of Training

As part of the training program for local elections officials, the WEC has created an election security training curriculum that focuses on a variety of election security issues. Various resources in this program have been developed and made available to local election officials through in person trainings, tabletop exercise (TTX), and online webinars and materials located in the WEC Learning Center.

a. Election Security Tabletop Exercises (TTX)

WEC staff attended an election security training and tabletop exercise hosted by the Defending Digital Democracy project at Harvard Kennedy School of Government's Belfer Center in the spring of 2018. At the event, WEC staff worked with election officials from across the United States to learn about election security best practices, as well as to participate in a tabletop exercise (TTX) that simulated potential real-life security-related events that could occur leading up to and including Election Day. The purpose of the TTX was to provide participants experience in election official roles different from their own and to make participants aware of the various types of potential incidents that could arise related to Election Day. These incidents were scripted and encompassed a wide variety of topics and severity, ranging from weather-related issues that could potentially impact polling places, to larger cyber security incidents that would require the assistance of IT professionals.

WEC staff saw value in participating in the TTX and concluded that Wisconsin county and municipal election officials would benefit from both the training and simulation exercise. WEC staff created an elections security train-the-trainer program, in partnership with Wisconsin county clerks, to reach our local election officials. The train-the-trainer program was designed to provide training and experience with election security materials to the county clerks who would then train their municipalities using materials and staffing resources provided by the WEC. The ultimate goal was to provide a safe, low-stress environment for participating election officials to test their election day emergency response plans against the incident injects to test the effectiveness of existing knowledge, policies, and practices as they relate to election security (operational, physical, cyber), provide an increased awareness and preparedness, and adapt and implement the training and lessons learned. The training was developed to encourage participants to work through the scenarios, to practice their communication plans, and to take action, without the risks or potential repercussions they may face in real life.

WEC staff created a second iteration of the election security TTX program and debuted it to clerks in August 2019. TTX 2.0 was created with the same goals as the first election security TTX program but includes new security incidents and situations. The addition of incidents allows for clerks who have already taken the first iteration of the election security TTX program to participate and interact with new situations. The injects allow for participants to work through cybersecurity, general security, and election administration issues in a low-stress environment.

All TTX materials were created with input from local election officials and have been well received and replicated for local TTX trainings. All training materials are now posted and easily accessible to clerks on the WEC Learning Center website.

b. Security Training Videos and Webinars

WEC staff has developed a series of webinars and videos for local election officials that focus on different aspects of elections security. The goal of these webinars is to bring all WisVote users up to a basic level of security knowledge. WEC staff published our security webinar series in two installments. The first installment of this series focuses on a broad introduction to security basics and resources. The second installment of security webinars provide more detailed information regarding specific cyber security topics – email security, web security, identifying phishing attacks, etc. The webinar stresses the importance of communicating any questions or concerns WisVote users might have to WEC staff so that any potential issue or situation can be quickly resolved. The goal of the WEC training initiative is to create a security campaign that resonates with all election officials and the public and can be more widely applied to other duties local election officials may have in their community.

The success of the WEC security training videos has gained attention in other states and on the federal level. Multiple states have either shown the WEC’s security training videos in their entirety or have used parts of the video series to inspire their own security training. In 2019, the WEC received a Clearie for Outstanding Innovations in Elections for its cyber security training program series. The Clearie awards highlight exemplary models which can serve as examples to other election officials and offices.

c. Security Checklists

Because many municipalities do not have access to IT resources, the WEC is also investigating options and feasibility for ensuring that all municipal clerks have access to IT best practices. WEC training staff is currently developing a series of cyber security checklists for local election officials that they can use to analyze whether their hardware and practices are secure.

Checklists being developed include:

- Is your IT secure? What IT resources are available?
- Is your polling place secure?
- Security starts on your personal device
- Minimum system requirements for devices used to access WisVote (operating system, browser, antivirus, etc.)
- Checklist for Ballot Security
- Election Day (polling place, voting equipment, etc.)
- After Election Day (canvass and voting equipment storage)

d. Other Training Resources

The WEC Training staff has also developed the following resources to train Wisconsin municipal clerks regarding election security:

- A survey of local election officials to establish a baseline and to better understand the election security challenges clerks face and the resources they may have available.
- An Election Day Emergency Response template for clerks to use to develop their own response plan for elections to ensure that the municipality is capable of conducting an election in the event of any potential threats and adverse conditions.
- Tip sheets on practices that can enhance security in elections.
- Lists of common security problems, vulnerabilities and troubleshooting.
- Updates of manuals and other guidance materials.
- Training agendas and supporting materials train election officials that can be counted towards required training hours.

2. Communications

a. Public Information Campaign

A concern for elections nationwide ahead of the 2020 cycle is the spread of misinformation. To combat the potential for misinformation to impact voters in Wisconsin, the WEC has launched a public information campaign to dispel election rumors, instill a greater trust in Wisconsin's elections, and position the WEC as the official source of truth for nonpartisan election information.

In August 2019, the WEC hired a professional advertising and public outreach organization to conduct market research on public perspectives concerning election security in order to successfully identify what concerns voters may have about election security in Wisconsin, as well to determine how to best reach these voters and the general public with effective messages. The agency is currently using the fall of 2019 to conduct qualitative and quantitative interviews and message testing. These interviews and testing events will determine if and how the WEC proceeds with a public information campaign ahead of the 2020 election cycle.

A condition for the public information campaign includes media training for both WEC staff and local elections officials. Part of this training will incorporate crisis communication assistance that can be used in an election security event, and will contain items such as sample holding releases, utilizing a communications team, and more.

b. Secure Communications Portal

Email communication is increasingly becoming a threat to election security. Phishing attempts through links and attachments can threaten the security posture of elections officials. In response, the WEC is creating methods to more securely communicate with clerks.

Currently, the WEC communicates with clerks through email and clerk communications that are posted to the WEC website. Due to the increased sophistication of phishing emails and spoofing attempts, the WEC is working to create an official communications feed accessible in WisVote that credentialed clerks could access. The WEC plans to have the secure communications portal implemented ahead of the 2020 election cycle.

c. RAVE Communication with Local Elections Officials

The RAVE emergency alert system provides election professionals statewide with real-time communications about emergencies and other situations that impact their jurisdiction's operations. RAVE supports many communication techniques including text messaging, voice telephone alerts, e-mail, and even social media. The system also supports limited two-way communications.

The WEC plans on implementing a RAVE alert system to provide another means to communicate urgent, time-sensitive, and actionable information to election officials across the state, whether they are full time clerks, or they are election inspectors who only work 4 election events in a calendar year. Currently, WEC staff is in the process of testing the RAVE system with a planned rollout in early 2020.

3. WisVote

WisVote is the State of Wisconsin's complete election management system. WisVote is a complex web-based application used to manage all aspects of elections administration including registering candidates, setting up elections and ballot styles, determining ward and district boundaries, maintaining voter registration records, issuing absentee ballots, and much more. WisVote is owned and operated by the WEC and is used by municipal and county clerks around the state. Both the Federal Help American Vote Act (HAVA) and Wisconsin State Statutes require the WEC to maintain a statewide elections administration system and for municipal and county clerks to use the state prescribed system to administer elections. The WisVote system was built in-house at the WEC, which is unique as many states contract with vendors to build statewide elections systems. Building the system in-house gives the WEC complete control over customizing the system for Wisconsin law and implementing security

measures that are compatible with the DET server security structure. The WisVote application was built using a highly customizable platform that includes many advanced security features.

While the WEC utilizes DET for server infrastructure and server security, the WEC is responsible for the security and maintenance of the WisVote application itself. The WEC sets permissions and policies for the WisVote system. The WEC also tests, maintains, enhances, and patches the application. In addition to the WisVote system, WEC also develops and maintains related IT applications such as the MyVote Wisconsin website and voter portal, the Canvass Reporting System, BadgerVoters, and more. The majority of the staff resources at the WEC are dedicated to the development, maintenance, training, and security of WisVote and its related systems. Security of WisVote and the data contained within are the paramount responsibility of the WEC. To protect WisVote and other WEC technology, the WEC is responsible for the following:

a. User Permissions and Distribution of Client Access Licenses

WisVote is built on a licensed software platform. The platform requires that each user of the system have an individual Client Access License (CAL) to access the system. This means that a CAL is required for each municipal and county clerk and any staff in their office who use WisVote. The WEC has made the decision to purchase CALS on behalf of the users of WisVote. This gives the WEC control over who has access to the WisVote system. The WEC has purchased 3,000 CALs to ensure that each clerk and member of clerk staff can have their own unique login. There are enough CALs for clerks to bring in additional staff to help with WisVote tasks during high turnout elections. As the owner of the CALs, the WEC is responsible for granting access and assigning permissions to each WisVote users.

Each user of the WisVote system is assigned a unique user login by the WEC Helpdesk. The user is then assigned system permissions by the WEC to control the user's access. Users are given the minimum amount of access required to do their job. For example, some users, like temporary clerk staff, are given read-only WisVote permissions so they cannot modify information. Other users, like municipal clerks, have permissions to enter voter information, modify existing information and perform administrative activities like setting up elections for their municipality. However, the municipal clerk's permissions are restricted to only their authorized municipality so that they are unable to see or modify records outside their jurisdictions. County level users have permissions for their municipalities to assist with data entry and to coordinate county-level responsibilities. Managing user permissions is an extremely important aspect of securing the WisVote system.

User credentials are also used to log each user's activity in the WisVote system. Logging user activity allows the WEC to monitor the entire system for unusual activity and to maintain a record of each change made to system data for security auditing. Monitoring activity also

allows WEC and DET users to see where the WisVote activity is coming from. WisVote is only available to users whose IP addresses are within the United States. IP addresses outside of the U.S. are blocked from the WisVote system. IP addresses from outside of the state of Wisconsin are also limited and flagged.

b. System User Policy

Currently, all users of the WisVote system are required to sign user agreements before they are given access to the WisVote system. The WisVote user agreement is prescribed and enforced by the WEC. The agreement contains important information about requirements for securely maintaining voter data which contains confidential information. The WEC revised the WisVote user agreement to include specific policy language regarding requirement for remote WisVote access, minimum hardware requirements, minimum software requirements, software restrictions, and the mandatory completion of WEC elections security training.

c. User Passwords

The WEC helpdesk manages passwords for all WisVote users. Once the WEC assigns a credentials to a user, the user then sets a unique password that periodically expires, which allows the user to create new, unique passwords on a regular basis. The password is required to be of a certain length with complex characters before it is accepted. Users set their unique passwords through an online, encrypted portal. The WisVote system uses the same login and secure password structure that is used by DET for all state users.

i. Multi-factor authentication

Multi-Factor Authentication (MFA) is a password security measure in which the user of a system must enter his or her username, password, and then a separate piece of information to authenticate identity and ensure that only authorized and credentialed WisVote users have access to the system. WEC staff has worked with DET to implement an MFA solution through the state IT enterprise for all WisVote users.

When implementing the MFA model for WisVote, WEC staff understood the scarcity of options experienced by some local election officials when it comes to IT resources and purchasing new security equipment. The WEC utilized funds from the 2018 HAVA election security grant award to purchase MFA devices, called FIDO keys, for every WisVote user in the state. Outside of the FIDO key, credentialed users have the option to receive a phone call with the second factor information they can then enter to access WisVote. These options were chosen to provide the greatest flexibility for users with different resources and setups while also accommodating the timeline of the MFA rollout.

WEC staff created multiple training documents and webinars guiding WisVote users through the MFA rollout. The WEC relied on county clerks to help distribute the original MFA devices to all WisVote users in their county and was successfully able to roll out a version of multifactor authentication to most WisVote users before the 2018 General Election. All WisVote users were enrolled in an MFA program by December 2018. WEC staff will continue to work with DET to offer accessible MFA options to securely access WisVote in the future.

ii. Password Recovery Process

The WEC also has a password recovery process in place. A WisVote user who forgets his or her password contacts the WEC Help Desk who will verify the user's identity and prompt the user to reset their password through a secure web portal. The user will not be able to access WisVote until he or she sets a new password that meets the minimum password complexity standards.

WisVote also contains an automatic password expiration process. User passwords expire at short intervals. Once users' WisVote passwords expires, they cannot access the WisVote system until they change their passwords using a secure web portal. The new password must be significantly different from previous passwords or it will not be accepted. An automatic password expiration process protects the system in case an unauthorized user gains access to a password because the unauthorized user would only have access for a limited time. WisVote users can also change their passwords at any time if they believe their password has been compromised.

The WEC is continuing to work with DET and other security partners to improve the password recovery process. As with any security measure, WEC will continue to implement new best practices as they become available.

d. Management of System Reports and Information

As the custodians of the Wisconsin statewide voter registration system and its data, the WEC has the responsibility of ensuring that voters' personally identifiable information is protected. Certain fields in each voter registration record are protected, such as date of birth, driver license number, and partial social security number. Users of WisVote, such as clerks and their staff, access this information for business purposes such as entering voter registrations. The WEC has put additional restrictions on the database columns that contain personally identifiable information to prevent them from being included in system reports. This will help to prevent the accidental release of personally identifiable voter information that could happen if a report were generated, printed and then discarded.

e. Systems Testing

i. On-staff Security Personnel

The Wisconsin DET has cyber security staff, including ethical hackers who can help agencies identify vulnerabilities in their system. While the WEC will work with DET cyber security staff to complete testing and vulnerability assessments, WEC has also made the decision to develop this expertise in-house with a staff member who is intimately familiar with the agency's custom IT solutions. To this end, a WEC staff member is working towards the Ethical Hacker certification to continue to complete penetration testing on agency systems and to focus on making security recommendations to improve Wisconsin's election systems security.

ii. CompTIA Security Certified Staff

The U.S. Department of Defense (DOD) requires all staff working in technical and managerial positions on systems with confidential or classified information to have certifications in how to prevent unauthorized access to information. The WEC is considering adopting these standards for our technical staff.

The DOD defines three broad categories that directly correspond to categories of Commission staff:

- Information Assurance Technician (IAT). This is an information services position that may make changes to configurations or updates to software. This corresponds well to the Commission's WisVote Elections Specialist positions. DOD requires IATs to have one of CompTIA's Security+, ISC²'s Systems Security Certified Practitioner (SSCP), CompTIA's Advanced Security Practitioner (CASP) or Certified Information Systems Security Professional (CISSP). Some of these are considered to be very advanced certifications and would require years of training or experience for staff to achieve, but the WEC is exploring requiring or encouraging staff to get either the Security+ or SSCP certifications.
- Information Assurance Manager (IAM). This is a managerial position that oversees IATs. This may be appropriate for the Commission's Assistant Administrator. The Security+ and CISSP would be appropriate certifications for this level as well, but Certified Information Security Manager (CISM) is probably a better fit.
- Information Assurance System Architect Engineer. This is a software engineer position that develops and maintains systems that process or contain confidential information. This corresponds to the Commission's developer contract positions. The most appropriate certification here would be the ISC²'s Certified Secure Software Lifecycle Professional.

The DOD also defines several smaller categories as classes of Cyber security Service Provider (CSSP). These do not directly correspond to any position currently used by the Commission, but there is significant overlap between the required training for these CSSP classifications and the classifications detailed above. Training for all of these federally recommended certifications is available to staff through FedVTE, discussed elsewhere in this document.

iii. Endpoint Testing

In order to understand the cybersecurity posture of Wisconsin's clerks, the WEC needs to understand what operating systems and security patches each and every WisVote user is using to access the system. As the WEC is not able to physically inspect all devices used to access WisVote, WEC staff has pursued a software option that will transparently report the status of the device accessing the voter registration system. Endpoint testing will allow the WEC to independently and accurately capture the state of a user's hardware and software over time. The local elections officials of Wisconsin have vastly different levels of knowledge and comfort with their IT system in their offices, and by creating a report of a clerk's current hardware and software situation, WEC staff can conduct targeted outreach to help that user become compliant before accessing WisVote.

In order to implement the endpoint testing, WisVote users will have to install the client on their device, which will report to WisVote that the device met the security policies before allowing it to access WisVote. Currently, WEC staff is developing training materials that will walk clerks step-by-step through the installation process to allow.

f. MyVote

The WEC's MyVote Wisconsin website is an extension of the statewide voter registration system. MyVote allows voters to register to vote online, find their polling place, view a sample ballot and more. The MyVote website is protected by the same DET server security structure as the WisVote system. Because MyVote is a publicly available site, there are some modified security measures in place as well as additional testing for the public facing portal.

Regular penetration testing is performed on the MyVote site to replicate hacking scenarios and attempt to identify vulnerabilities. The site regularly passes penetration testing by state testers and scores very highly on DHS scans. In addition, the WEC has placed many throttling measures on the website to stop extraneous activity. Throttling measures slow down malicious actors and "bot" activity by fractions of a second, enough to stop attack but not enough to slow services of legitimate users. There are additional checks and stops in place to prevent multiple transactions from being completed using the same voter information. Also, while MyVote facilitates services like absentee ballot requests, the requests are ultimately emailed and

processed by the municipal clerk. This human driven end process ensures that there are checks and balances in the process and that only eligible voters receive a ballot.

4. Servers

a. Patching (In-house schedule vs. DET)

In addition to the patching services provided through DET, WEC also conducts patching on agency systems. These are additional patches to those deployed by DET that are specific to elections applications. Maintaining some patching responsibilities affords the WEC additional control over when a patch is implemented and allows the agency to minimize any potential impact on our systems. Using this method, the WEC can implement an emergency patch on a testing server and then analyze its impact before rolling it out to the live WisVote system. The goal is to ensure that the elections systems are kept as up to date as possible with the best information and fixes but to also implement these fixes in a responsible way that does not impact clerks or voters who are using our system. Outages can undermine user confidence in the WisVote system and voter confidence in the election process, so it is very important to be strategic about testing and deployment.

b. Encryption of Data at Rest and in Motion

The WEC is implementing protocols to encrypt the data on agency applications. All elections data stored in application databases is encrypted through DET's server hosting. Additional encryption measures are being deployed to provide another layer of protection, including encryption of confidential data on WEC in-house applications before being stored in the database server at DET. WEC and DET are also exploring additional opportunities to encrypt data as it is "in-motion" or as it is moving between applications. Encryption is an important aspect of election security. However, encryption can have negative performance impacts that may present a challenge for clerks and voters using WEC systems. WEC staff is working closely with the in-house development team and DET to find the correct balance for Wisconsin elections administration.

c. Nightly Comparisons of Database Changes

To monitor activity in the statewide voter registration database, WisVote, the WEC is continuing to build on its process for logging all system events and analyzing the logs for unusual activity. WEC staff is then able to compare data each day to the backup data from the day prior to identify changes made within the system. Once a list of changes is identified, the log data can then be analyzed to flag unusual activity. System activity will be flagged as unusual if it deviates from the baseline system activity in a meaningful way. For example, if 1,000 voter

registrations are submitted in a town of 800 voters, the system and WEC staff would flag this activity as unusual and contact the appropriate DET, federal, and local contacts to investigate the activity. There are also software tools available to help analyze system log data that the WEC is exploring in conjunction with DET.

5. Voting Equipment

a. State Testing and Certification

On the federal level, the U.S. Election Assistance Commission (EAC) provides testing and certification of electronic voting systems. Each system approved for use is reviewed by an independent testing authority to ensure that the functionality, security and accuracy meets federal standards. The Wisconsin Elections Commission conducts an additional testing and certification process designed to assess whether a system is compatible with Wisconsin election law. Each system is tested to confirm that it is able to be programmed to accommodate election configurations unique to Wisconsin. State law requires that three different election types are tested, and a set of marked ballots is processed on the equipment to ensure accurate tabulation. In addition, state certification requires isolating voting system components from internet connectivity to prevent remote access to the system.

b. Audits

Wisconsin Statutes require a post-election audit of the performance of each voting system used in the State of Wisconsin. The audit is designed to assess how electronic voting systems performed on Election Day through a hand-count of electronically tallied ballots. The audit is required following each General Election.

After the 2018 General Election, 5% of all reporting units were randomly selected to be audited. A representative sample of reporting units that use each type of voting equipment are included in the selection process. The audit also selects at least one reporting unit from every county to ensure the audit has a statewide reach. The highest office on the ballot is included in the audited contests and three other statewide contests are drawn by lot.

During this process, two elections workers conduct an independent hand count of paper ballots and tally the results of the contests being recounted. The individual tallies are compared to each other and any discrepancies are resolved before an agreed upon final hand-count tally total is determined. If the hand counts differ from each other, the paper records/ballots must be recounted. The final hand-count tally total is then compared to the Election Night results tally tape and discrepancies are noted.

The audit is considered a public meeting and proper notice shall be posted or published at least 48 hours in advance. Each audit is required to be completed prior to the certification of the election by the WEC and a report on the outcome is prepared by Commission staff. Audit materials are submitted to the WEC for review and Commission staff may request that a vendor investigate and provide explanation for any unexplained differences between the voting equipment tally and the paper record tally.

Based upon the results of the audit, the WEC may, at its sole discretion, choose to re-test the voting system per WEC Chapter 7 of the Wisconsin Administrative Code. The test is a condition of continuing approval of the voting system and is designed to ensure that voting systems approved for use in Wisconsin continue to adhere to the terms of their state certification.

6. Election Night Reporting/Canvass

a. System Security and Training

The WEC does not report Election Night results, the statutory responsibility for reporting Election Night results rests with the county and municipal clerks. Wis. Stats. §§7.51(4)(c) and 7.60(1). The WEC staff provide technical and business process support for clerks reporting Election Night results.

Sixteen of the 72 counties use the WEC Canvass Reporting System to collect vote totals from the municipalities and to generate the reports used for Election Night results. The Canvass Reporting System is a web-based application maintained by the WEC where clerks enter results for each voting precinct (reporting unit). WEC staff provide IT support for the counties using the WEC Canvass Reporting System to report Election Night results. Staff ensure this system is available and functioning throughout Election Night and often into the early hours the day after Election Day. The remaining counties use local IT or vendor purchased systems to produce Election Night result reports.

After certification by county boards of canvassers, counties use the Canvass Reporting System to transmit official canvass results for federal and state contests to the WEC. When canvassing federal and state offices, the WEC Canvass Reporting System must be used to transmit the official results data electronically to the WEC. County clerks manually enter results for federal and state contest into the Canvass System or upload a results file from a vendor purchased election management software (EMS). The County Board of Canvassers carefully reviews the election returns and prepares the official canvass statement that contains the Tabular Statement of Votes Cast, the Summary Statement and the Certification. All three sections are produced from the WEC Canvass Reporting System.

An original signed Summary Statement and Certification of the Board of Canvassers is printed from the WEC Canvass Reporting System, checked for accuracy and signed by the Board of Canvassers, scanned, emailed and mailed to the WEC. The Summary Statement and Certification cannot be printed from the WEC Canvass Reporting System until the county clerk electronically submits the official results, once electronically verified the WEC Canvass Reporting System locks the data from being edited. WEC staff verifies that the signed Certification matches the verified results in the WEC Canvass Reporting System. WEC staff compare the Certification time stamp and result information with the system log to validate that the printed results have not been altered after the results were officially verified. Only WEC staff can reject or unlock the electronically verified county results. If a mistake is identified after verification, WEC electronically rejects the results and the county must electronically verify the corrected results and print and sign a new Summary Statement and Certification to deliver to the WEC.

After each county board of canvassers delivers its official results, the WEC uses the Canvass Reporting System produce the official results reports which are used for certification and posted to the WEC website.

7. Legal Infrastructure

Contingency planning and emergency responses may be necessary either because of activity specifically intended to disrupt voting and elections systems or, more likely, because of an unrelated situation or condition which incidentally impacts voting or the public on a local or regional level. As part of the agency's election security planning, WEC management and Staff Counsel have reviewed the legal framework for invoking and exercising emergency government powers.

Wisconsin's elections agency has occasionally assisted local election officials during various emergency situations affecting an election, such as inclement weather, a bomb scare, or traffic accident that affects access to a polling place. On Election Day, when a polling place has been closed for an extended period of time due to an unexpected incident or emergency, agency staff has assisted municipalities which have sought a court order to extend polling hours. To address such situations, the WEC maintains sample court filings so that documents can be prepared quickly, if necessary, on Election Day, and has provided local election officials with sample templates they can use when consulting with their circuit court judge and the WEC to determine if an extension of polling hours is appropriate.

The WEC has also focused on training and coordination with agencies observing and responding to events that occur on election day at the polls, including discussion of the legal authority for intervening and responding to various scenarios. In conjunction with the Wisconsin

Department of Justice and the Milwaukee County District Attorney's Office, agency staff has consistently conducted webinars for law enforcement agencies and prosecutors that have personnel in the field across the state on Election Day.

Prior to the 2018 General Election, the WEC coordinated a preparedness meeting with representatives from key federal and state offices to ensure cooperation and coordination of response to potential incidents affecting elections or voting. Representatives from the Federal Bureau of Investigation, Department of Homeland Security, U.S. Department of Justice, Wisconsin Department of Justice, Wisconsin Emergency Management, Wisconsin Department of Administration, Division of Enterprise Technology, and Milwaukee County and Dane County District Attorney's offices along with the WEC, participated in meetings to discuss the roles that each office could provide and to work through hypothetical scenarios and the proper approach to a coordinated response consistent with federal and state laws.

The WEC intends to continue its partnership with federal and state offices to conduct training and provide information on best practices for responding to potential incidents leading up to and on Election Day. Agency staff will also continue to prepare plans and documentation related to the legal aspects of incident response with these offices, and more detailed information will be provided to the Commission within the second section of this Election Security Plan.

a. Statutory References

Wis. Stat. §§ 323.01 (1) and 323.10 provide the Governor the legal authority to declare a state of emergency to respond to events that have already occurred, or to respond to imminent threat of a disaster. In addition to the state's response through the Governor's office, Wis. Stat. §§ 323.14 and 323.15 spread the responsibility of responding to and planning for potential emergencies to counties, cities, village and towns across the state. An emergency declaration establishes specific temporary duties and powers to the Governor, state agencies and local officials, which will be further outlined in the Response section of this Plan.

The WEC is working with Wisconsin Emergency Management to develop a template for an emergency order that could be issued related to election infrastructure or processes. Agency staff has also communicated the importance of incident response planning to local election officials and encouraged them to consult with local and regional law enforcement and emergency management personnel.

b. Implementing Legislative Changes

During the process of its election security planning, WEC staff is assessing whether any existing statutes need to be amended to accommodate risk prevention and incident response. If

necessary, staff will work with the Legislature, Wisconsin Emergency Management, and the Governor's Office to develop legislation to enhance election security and response capability.

The WEC's current legislative agenda requests that the Legislature amend Wis. Stat. § 6.96 to allow state courts to issue orders to allow individuals to vote after the normal polling hours pursuant to an order. The statute currently specifies that a federal court may issue an order to extend polling hours. In such situations, municipalities have filed petitions with state circuit courts which have exercised their inherent authority and agreed to limited extensions, especially when no party objects to the request.

8. Elections Security Committees and Councils

In spring of 2019, the WEC consulted the Wisconsin County Clerk's Association, the Wisconsin Municipal Clerk's Association, the Wisconsin Town's Association, and a list serv of all clerks in Wisconsin to ask for volunteers to serve on an Election Security Clerk Advisory Committee. The WEC recruited 17 county and municipal clerks from a variety of jurisdictions to serve on the committee.

The goal of the Election Security Clerk Advisory Committee is to involve local elections officials at the beginning of WEC projects to better tailor agency efforts to support the needs of the local election officials throughout Wisconsin. The WEC will continue to solicit the knowledge and opinions of local election officials ahead of the 2020 cycle.

a. Election Security Clerk Advisory Committee

In spring of 2019, the WEC consulted the Wisconsin County Clerk's Association, the Wisconsin Municipal Clerk's Association, the Wisconsin Town's Association, and a list serv of all clerks in Wisconsin to ask for volunteers to serve on an Election Security Clerk Advisory Committee. The WEC recruited 17 county and municipal clerks from a variety of jurisdictions to serve on the committee.

The goal of the Election Security Clerk Advisory Committee is to involve local elections officials at the beginning of WEC projects to better tailor agency efforts to support the needs of the local election officials throughout Wisconsin. Currently the Committee convenes public meetings once-a-month to review current security projects, discuss priorities, and offer suggestions. The WEC will continue to solicit the knowledge and opinions of local election officials ahead of the 2020 cycle.

b. Election Security Council

In addition to the advice and input received from local elections officials with the Election Security Clerk Advisory Committee, the WEC has worked to coordinate input and communication between the various election security partners in state government. In order to increase communication and coordination ahead of the 2020 elections, the WEC has created an Election Security Council with representatives from the following offices:

- Federal Bureau of Investigation (FBI)
- Governmental Information Processing Association of Wisconsin (GIPAW)
- League of Wisconsin Municipalities (LWM)
- Office of Governor Tony Evers (Governor's Office)
- U.S. Department of Homeland Security District V (DHS)
- Wisconsin Assembly Committee on Campaigns and Elections (Assembly)
- Wisconsin Counties Association (WCA)
- Wisconsin County Clerks Association (WCCA)
- Wisconsin Department of Justice (DOJ)
- Wisconsin Department of Military Affairs (DMA)
- Wisconsin Department of Transportation (DOT)
- Wisconsin Division of Enterprise Technology (DET)
- Wisconsin Elections Commission (WEC)
- Wisconsin Emergency Management (WEM)
- Wisconsin Municipal Clerks Association (WMCA)
- Wisconsin Senate Committee on Elections, Ethics, and Rural Issues (Senate)
- Wisconsin Statewide Intelligence Center (WSIC)
- Wisconsin Towns Association (WTA)

The members of the Election Security Council will meet every meet approximately every 60 days starting in fall 2019 to share information related to election security matters.

E. County Level

Wisconsin elections administration is decentralized. Each town, village, and city has an elected or appointed clerk who oversees elections for the municipality. However, Wisconsin's 72 County clerks also play a vital role in the administration of elections and have unique elections responsibilities outlined in state statutes. County clerks are an important partner in elections security as they are often the conduit for information from the WEC to Wisconsin's 1,852 municipal clerks. Wisconsin's 72 county clerks have the following roles and responsibilities in securing Wisconsin elections:

1. WisVote

a. Hardware & Software Requirements

Like state users and municipal clerks, counties should maintain minimum hardware and software requirements on devices used to access WisVote and elections information. While most counties have IT support available, the WEC will provide counties with the same training and resources that are made available to municipalities. County clerks will be able to use WEC checklists and training to analyze county technology and then work with their IT team to upgrade hardware and software to ensure it meets security standards.

b. Staff Security Measures

The WEC has also provided counties with elections security training using the same process and curriculum outlined below for municipal clerks. It is the county clerk's responsibility to ensure that the elections staff in their office is operating securely. Some counties may wish to implement their own security training for county and municipal staff.

c. WisVote Provider/Relier Relationship

Some counties provide election administration support to municipal clerks by entering voter data into the WisVote system on behalf the municipality. Municipalities who do not have the resources to enter information into WisVote themselves contract with the county clerk for those services. In these instances, the municipality tracks election related information, such as absentee ballots and voter registration data, using a paper log. The log is then transmitted to the county clerk, who enters the information into WisVote. In these situations, the county is responsible for executing an agreement with the municipality that includes the secure transmission of elections materials between the municipal and the county.

When a county is granted access to WisVote on the behalf of a municipality, the county clerk becomes the custodian of municipal voter information and the county becomes responsible for the security of municipal election information. WisVote responsibilities can sometimes be shared between municipal and county offices, and the WEC has provided security training and resources to election staff at both levels.

2. Voting Equipment

a. Programing of Voting Equipment

County staff or voting equipment vendors are responsible for programming voting equipment so that ballots are accurately created and tallied for each election. All voting equipment

memory devices should be programmed using a computer that is not connected to the internet. They should also be assigned a unique serial number and stored in a secure location that only the clerk and approved staff can access between elections. Chain of custody documentation should be maintained for the transfer of memory devices to and from the programming entity (county or programming vendor) to the municipality. The WEC is developing the administrative rule that details chain of custody procedures for voting equipment memory devices and will continue the process for approval of the rule until it is adopted.

b. Storage of Equipment Between Election

All voting equipment should be stored in a secure location between elections. Access to the storage location should be restricted to prevent unauthorized access to the equipment. A list of people who have access to the equipment should be kept to ensure that access to the storage area can be monitored. In addition, any computer where election management software is located should not be connected to the internet between elections. These devices should only be used to operate the electing management software and all other non-essential applications and program should be removed from the device.

3. Election Night Reporting/Canvass

a. Posting Unofficial Results and Entering Results into Canvass System

Counties are required to post “unofficial” results on Election Night. Wis. Stats. §§7.51(4)(c) and 7.60(1). The unofficial Election Night returns must be posted by county clerks two hours after receiving them from the municipalities. The results must be reported by ward or reporting unit and must include results from all contests including municipal contests, school district contests and contest for special districts such as sanitary districts.

Counties receive unofficial results from the municipality or ward inspectors by a variety of methods. Unofficial results may be transmitted by modem, fax, email, hand delivery or by telephone. The county may use election night reporting software purchased from a vendor to post reports on the Internet. Many utilize systems created by their county IT staff for Election Night Results reporting. The WEC is responsible for posting a link on its website to each county’s election night results. The key to successful Election Night reporting is to establish internal office procedures for Election Night reporting well in advance and have adequate staff available on election night for receiving, entering and proofing Election Night results.

The outcome of the election is not official until the completion of the canvass. The canvass is the compilation of election returns and validation of the outcome that forms the basis of the official results. The county clerk and two qualified electors of the county appointed by the clerk constitute the county board of canvassers. The purpose of the county board of canvassers is to proof the returned results from the municipalities for accuracy, certify the results of elections and make the official determination of election or primary winners within county reporting units for county, state and federal contests. The county board of canvassers files one complete certified canvass statement in the office of the county clerk or board of election commissioners. When canvassing federal and state offices, the WEC Canvass Reporting System must be used to transmit the official certified results data electronically to the WEC.

County clerks then manually enter and certify their results for federal and state contests into the WEC's Canvass System or upload a results file from a vendor-purchased election management software (EMS). An original signed Summary Statement and Certification of the Board of Canvassers is printed from the WEC Canvass Reporting System, signed by the board of canvassers, scanned, emailed and mailed to the WEC. It is the county clerk's responsibility to ensure that official election totals are accurately certified and entered into the WEC's canvass reporting system. While errors made in the canvass reporting system can be corrected by WEC staff, publicly reported errors in the certification and reporting can undermine the public confidence in the elections process and all precautions should be made by the county to avoid them.

F. Municipal Level

The structure of elections administration is unique in Wisconsin compared to other states. In Wisconsin, elections are administered at the municipal level, meaning that each town, village, and city administers elections, whereas most other states administer elections at the county level. In Wisconsin, there are 1,852 municipal clerks who conduct elections. Most other states have between 50-100 county clerks who conduct elections. This unique structure can be both a benefit and a challenge. It is a benefit because municipal clerks have a close, local relationship to their voters and their needs. It can be a challenge to ensure that each municipality has the training and resources to conduct elections in a consistent and secure manner. The following sections outline the roles and responsibilities of municipal clerks in elections security.

1. WisVote

a. Hardware & Software Requirements

Many town and village clerk offices in Wisconsin do not have in-house IT services or support. Some towns in Wisconsin do not have internet connections available for clerk staff. Other

Wisconsin municipalities do not provide an official office computer to the clerk staff. Some clerks are therefore required to access official clerk business using a home computer, a computer in a neighboring community, or a public computer at a library or school. The WEC recognizes these challenges faced by municipalities and it attempts to bridge the gap by providing IT resources and best practices.

While municipalities may face challenges in obtaining the necessary IT support, they still have a responsibility to ensure that they are accessing elections systems and information in a secure manner. The WEC has issued guidance for municipalities regarding minimum hardware and software requirements for accessing the WisVote systems, as well as a memo to municipal governing bodies reiterating the clerk's need for these minimum hardware and software requirements. Municipal clerks can then use this guidance and memo to petition their governing bodies to budget for and provide the necessary software and hardware. Outdated, unsupported or un-patched hardware and software is a vulnerability to the elections system as a whole. It is municipal clerks' responsibility to ensure that they are accessing elections systems and data using secure channels.

The WEC has developed checklists for municipal clerks to use to determine if they meet minimum hardware recommendations. The checklist gives recommendations for purchasing new hardware to ensure a secure system. In addition to hardware requirements, the checklist includes items to analyze the operating system of the device to ensure it is patched and supported. In addition, the WEC has created a user agreement for the WisVote system that include minimum hardware and operating system requirements. Before a WisVote user is given credentials to the system, the user would need to commit to maintaining secure hardware and operating systems on the device used to access WisVote and complete a webinar training that details good cyber hygiene and security tips.

b. Staff Security Measures and Multi-Factor Authentication

Often municipal offices have multiple staff members who work in elections and within the WisVote system. The WEC has purchased licenses for the WisVote system to account for not only the municipal clerks themselves but for additional staff in each clerk office. Therefore, clerks and clerk staff should never share passwords to access elections systems, including WisVote. If a new staff member needs access to the WisVote system, the clerk should call or email the WEC helpdesk to obtain credentials for the new staff person. If a staff member leaves the clerk's office or no longer needs access to the WisVote system, the clerk should contact the WEC helpdesk immediately to notify it of the change.

It is the clerk's responsibility to ensure that their WisVote access credentials are protected and secure and that only necessary staff have access to the system. Login credentials are not only

used to maintain secure access for each user, but they are also used to track the WisVote activities of each user. WisVote maintains logs of user activity so that activity can be audited and analyzed to ensure security.

In addition to working to protect WisVote user credentials and passwords, the WEC implemented Multi-Factor Authentication for all WisVote users in 2018. Multi-Factor Authentication (MFA) is an important technology for preventing malicious access to user accounts. Proper implementation of MFA can prevent an attacker from gaining access to a user account, even after one has stolen the user's password. WEC staff rolled over 2,500 WisVote users into the MFA program prior to the November election.

Currently, WisVote users have an option to use an automated telephone call back to the specific clerk's phone number on file with the WEC to get a randomly generated code, or they can use a WEC-provided FIDO key. A FIDO key is similar to a USB drive which is inserted into a computer port and registers the user's touch to unlock access to WisVote. The keys are the most secure method, and for most users, the most convenient. To that end, staff procured 3,000 keys and distributed them to all the municipalities that use WisVote.

c. Managing and Entering Voter Information for Municipality

Municipal clerks are also responsible for entering and maintaining records for their voters into the statewide voter registration database, WisVote. The municipal clerk is the custodian for voter information. The clerks maintain their voter records using both the WisVote system and through the maintenance of paper records. Some municipal clerks do not use the WisVote system and rely on the county or a neighboring community to enter their voter information into the WisVote system on their behalf.

It is the municipal clerk's responsibility to securely maintain voter records in the system, to secure and maintain paper documents regarding voter information, and potentially to transmit voter information securely to their WisVote provider. The WEC provides training and guidance to municipal clerks on each of these responsibilities and it is the clerk's responsibility to complete this training and to maintain voter records in a secure and confidential manner and in accordance with state law and WEC guidance.

2. Electronic Poll Books

a. Hardware & Software Requirements

E-poll book hardware is dedicated hardware that can only be used as an e-poll book device. E-poll book hardware is stored securely, similar to other voting equipment. Should the hardware fail on Election Day, each polling location using e-poll books must be ready to switch to pre-

determined contingency plan, and these polling places have been instructed to have a paper copy on hand that can quickly be deployed to continue to process voters.

E-poll book hardware has required lockable ports and the WEC is working to implement another factor, such as a thumb print or smart card, to access the device. Currently, clerks and election inspectors will be required to enter a unique username and password, with the goal that an additional factor to access the e-poll book software will be deployed in the future.

b. Staff Security Measures

WEC staff has made several decisions regarding the e-poll book system being developed with the goal of reducing opportunities for interference or access to voter data by unauthorized actors. Only the necessary voter data required to check in an elector is included on the data load into the poll book device. This information will not include confidential data such as birth dates for voters who were already registered before Election Day. The e-poll book software and devices will also be kept offline. Polling places where multiple e-poll books are used may need a local network so that the e-poll books can share data, but they will not be connected to the internet.

Staff will run penetration testing sessions against the program and equipment to ensure that measures designed to defend against a hack operate effectively.

3. Voting Equipment

a. Initial Logic and Accuracy Testing of Voting Equipment Programming

All municipalities are encouraged to conduct logic and accuracy testing of their voting equipment programming after programming of the memory devices is completed. This testing is designed to confirm the accuracy of the programming and ensure the equipment is correctly reading ballots and tabulating votes. This testing is conducted before the public test of voting equipment, so that any programming errors can be remedied before Election Day.

b. Public Test of Voting Equipment

All municipalities are required to conduct a public test of their voting equipment before each election. This event is considered a public meeting and must be noticed at least 48 hours prior. The public test must take place no earlier than 10 days prior to Election Day and the public is invited to attend and observe the testing process.

Programming and functionality are verified by feeding a set of pre-marked ballots, or test deck, into the machine and reviewing the results tape that is generated at the end of this process. The test deck should include ballots with votes for all candidates and contests on the ballot. It is recommended that the test deck used for the public test differ from the test deck used by the programmer so that any errors in programming do not remain undetected. Vote totals for each candidate in a contest should differ so that votes transposed between candidates in a contest can be detected.

The public test ensures that paper ballots can be read by the optical scan voting equipment, all ballot contests are tabulating properly, voters are not allowed to exceed the maximum number of choices per contest, write-in votes are properly identified, and touchscreen voting equipment is programmed to capture voter intent. An errorless count is required after the process and any anomalies identified in this testing must be remedied before the equipment can be approved for use in the election, according to Wis. Stats. This process also adds transparency to the election process by allowing any member of the public to observe the operation and accuracy of the voting equipment prior to each election. Such transparency serves as an additional component of election security and factor in promoting public confidence in voting equipment and election results.

G. Poll Workers and Other Local Users

Wisconsin law refers to poll workers as election inspectors. Election inspector responsibilities regarding election security occur mostly on Election Day itself. Inspectors are responsible for conducting elections at the polls on Election Day. This includes processing and securing voter registrations, ensuring the process to receive a ballot is followed (photo ID, poll books, issuing voter numbers), ensuring each voter is at the correct polling place and receives the correct ballot, troubleshooting polling place issues, setting up and maintaining voting equipment, tallying ballots, and much more.

Election inspectors may work as little as two times every two years, or as often as four times each year. Regardless of how often they serve, inspectors need to maintain the same amount of training and knowledge. Each polling place is required to have a chief election inspector, who is ultimately in charge of administering elections at that polling place. If an incident occurs at the polls that requires law enforcement, the chief inspector is required to work with law enforcement to remedy the situation.

1. Voting Equipment

Following the public test, the voting equipment and all associated memory devices are required to be secured. A chain-of-custody log is required to be maintained that documents any access

to or transfer of each memory device. These procedures are intended to protect against malicious breaches to electronic voting equipment components as well as provide transparency regarding authorized access.

The memory device should remain in the machine and a tamper-evident seal should be used to secure the compartment that houses the memory device. Each tamper-evident seal should contain a unique serial number and that number should be recorded on the Inspectors' Statement along with other voting equipment security-related information. Verification of the serial numbers should take place before the polls open in the morning and after the close of polls. It is also recommended that election workers verify this information at several other points on Election Day.

The purpose of these procedures is to ensure that the integrity of the memory device is not compromised after the conclusion of the public test up until votes are tabulated after the close of polls. All instances of access to the memory device must be documented on the Inspectors' Statement and each memory device should remain secured after the election.

Voting equipment is not connected to the internet and any modeming capability is disabled until the polls close and the machine is in a post-election setting.

2. Electronic Poll Books

The WEC has created an electronic poll book, called Badger Book, in-house for use by municipalities across the state. The associated software program and training have been developed with the expectation that the main users of the Badger Book system will be election inspectors. They are responsible for using Badger Books in a way that maintains security standards on Election Day. While the WEC has developed the software and worked with the municipal clerk to configure the hardware, election inspectors will be operating the Badger Book. Login credentials will need to be maintained and safeguarded by those users.

The WEC has incorporated credential security into the Badger Book login process. Inspectors currently need to enter a unique username and password. In the future, the WEC aims to have a second authentication factor to ensure that only the authorized user has access to the Badger Book. The Badger Book also utilizes the login credentials and permissions to log activity by each user so that it can be audited post-election.

3. Polling Place Incidents and Disaster Response

Poll workers, namely the chief election inspector of each polling place, oversee the security of the polling place and for knowing the disaster recovery process for their polling place. Poll workers must receive training on polling place security, disaster response, and contingency

planning. Poll workers are responsible for contacting the appropriate authorities should there be an incident or disaster that impacts their polling place. The WEC is currently working with municipal clerks to incorporate election security training in already existing election inspector training.

H. Public Level

Voters, voter advocacy groups, and the media also play an important role in elections security. It is important for voters to understand the process and know what to expect when voting in Wisconsin. Therefore, it is the WEC's responsibility to partner with municipal clerks, voter advocacy groups, and the media to provide information to the public on elections security.

1. Voter Education and Preparation

The WEC is formulating a voter outreach and media plan for elections security. It is important that voters know where to find official information on the elections process and elections security. Informed voters can identify suspicious or unlawful elections activity and notify the proper authorities. Misinformed or uninformed voters may be unable to recognize or report legitimate election security concerns. WEC staff has worked with officials at major social media companies to quickly communicate any attempts to misinform voters and to have the offending posts removed. The WEC often partners with community groups and the media to distribute official information to the public. The WEC will continue to work with these partners to develop an effective messaging campaign about elections security. The WEC will also continue to create consistent message branding and verification methods so that voters know the information is from a trusted source.

While maintaining transparency in the election security process is a top priority, that priority must also be balanced carefully with the need to secure elections and not create vulnerabilities. The WEC has developed a communication strategy that keeps the public informed about elections while continuing to protect information that could be exploited by malicious actors. This communication strategy will be reviewed frequently to ensure necessary updates are made. The WEC partners with DET and DHS before releasing elections security information to the public. WEC asks DET and DHS to review such communications prior to release to ensure that sensitive or classified information is not disclosed.

Section II: Election Security Incident Response and Communications

A. U.S. Government Level

The designation of election systems as a critical infrastructure component by the Department of Homeland Security has increased the resources available for state at the federal level. The Wisconsin Elections Commission has continued to work with federal election and security partners to further prevent malicious attempts to compromise the election process and systems in Wisconsin.

The new federal designation for election systems have allowed for select members of WEC staff to have the security clearance needed to be briefed on classified information from the Department of Homeland Security. The designation has also helped to create new lines of communications that have allowed the Wisconsin Elections Commission to develop contact plans and procedures should there be an incident requiring federal assistance.

1. Monitoring Threats and Alerting States

Currently, three WEC staff members have received a security clearance from the Department of Homeland Security, allowing them to be briefed on classified information concerning election systems and election security.

Outside of classified communications, the Wisconsin Elections Commission is a member of the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC). The purpose of the ISACs are to quickly help spread information concerning election security around to elections officials across the United States. The WEC has procedures in place to contact members of the MS-ISAC and EI-ISAC should there be a need to alert election officials outside of Wisconsin about an election security issue.

Sample Situation: A notice from the Department of Homeland Security alerts the Wisconsin Elections Commission that multiple states have seen a rise in attempted cyber security incidents through the EI-ISAC.

Resolution: WEC staff will coordinate with appropriate state and federal agencies to research the issue and determine how to best prevent such incidents from occurring in Wisconsin or how to best respond if a cyber security incident has occurred. WEC staff

will also pass along any necessary information to other state and local partners as needed.

2. National Emergency Management

In the event of terrorist activity or a widespread national emergency, the Federal Government may have a preliminary plan in place for moving activities of election days. All elections will continue unless Federal or State officials have ordered otherwise.

Sample Situation: A national terrorist event/widespread emergency has occurred on Election Day.

Resolution: WEC staff will coordinate with appropriate federal agencies and the Governor of Wisconsin to receive guidance on how to proceed and will communicate any federal or gubernatorial decisions to local election officials.

B. National Elections Level

There are several national organizations that aim to coordinate professionals from across the country on important topics related to elections. The National Association of State Election Directors (NASED) is an organization comprised of the chief election official from each state. NASED coordinates conferences, events and communications to its members on important elections information including elections security. NASED coordinates information sharing among state election directors so that all states can benefit from best practices and lessons learned.

Organizations such as the National Association of Secretaries of State (NASS) and the National Association of State Chief Information Officers (NASCIO) are also involved in elections related matters. The WEC has reached an agreement with NASS to subscribe to its election related services and resources for a reduced membership rate. NASCIO is also an important election security partner, as many states, including Wisconsin, rely heavily on the office of the state Chief Information Officer to provide front line defense for election systems and servers.

1. Alerting States of Known Threats

Sample Situation: A national elections organization notifies the Wisconsin Elections Commission that multiple states have seen a rise in attempted cyber security incidents.

Resolution: WEC staff will coordinate with appropriate state agencies to research the issue and determine how to best prevent such incidents from occurring in Wisconsin or how to best respond if a cyber security incident has occurred. WEC staff will pass along information to the local election officials if it is deemed beneficial or necessary.

C. State of Wisconsin Enterprise Level

The Wisconsin Elections Commission (WEC) is an agency within the State of Wisconsin government. While the WEC is an independent state agency, it utilizes enterprise level technology services available through the State of Wisconsin Division of Enterprise Technology (DET). DET, housed within the Wisconsin Department of Administration (DOA), provides many services to the WEC including server hosting and management, phone and email hosting, and desktop imaging and support. The WEC also has other security partners at the state enterprise level including Division of Emergency Management, the National Guard and state and local law enforcement. In preparing for an election related security disaster or emergency management event, the National Guard and State level law enforcement have been able to provide resources and guidance. The WEC communicates regularly with state level enterprise partners and has regular meetings with such agencies to better understand and coordinate their roles in elections security prevention and response.

1. Alerting Agency to Known Threats

WEC staff work with DET staff on a regular basis. The WEC and DET both are members of the MS-ISAC and EI-ISAC. WEC staff alert DET staff when suspicious cyber activity is noticed by any WEC staff members. DET alerts the WEC about suspicious cyber activity that might be occurring with other state organizations that could potentially impact WEC systems or create a security incident.

2. Organization of Fusion Center

The National Network of Fusion Centers was created in the wake of the September 11, 2001 terrorist attacks to improve communication and coordination between national, state, local and private organizations. These centers provide central locations where members from multiple agencies work alongside each other, developing strong working relationships and fast pathways for communication between organizations.

There are two Fusion Centers in Wisconsin: The Southeastern Wisconsin Threat Analysis Center (STAC) in Milwaukee and the Wisconsin Statewide Intelligence Center (WSIC) in Madison. The STAC focuses on the urban areas of Milwaukee and its environs, while the WSIC focuses on the rest of the state. Because of its location in Madison, the WEC works most closely with the WSIC, but the WSIC works closely with STAC so communication flows wherever it is needed.

3. Wisconsin Emergency Management

Wisconsin Emergency Management is a division of the Wisconsin Department of Military Affairs that takes an all-hazards approach to emergency planning and response. WEM regularly assists localities with emergencies related to natural disasters and industrial accidents. As such, they have a 24/7 infrastructure in place for emergency response.

4. State Server Isolation, Load Balance, and Recovery

DET follows industry best-practices for a high-availability, multi-tenant network of data centers. Using a virtualized network of servers, they are able to provide dynamic load-balancing, and redundancy across geographically disparate data centers. In addition, they provide regular off-site backups. WEC presently takes advantages of these systems to provide availability of greater than 99.5% for critical systems. However, WEC plans to take better advantage of these systems in the future, along with better internal processes, in an effort to create an even more available and resilient system.

D. State Elections Level

The Wisconsin Elections Commission is made up of six members appointed by legislative leaders and the Governor of Wisconsin. The Commission staff is nonpartisan and is charged with administering and enforcing the election laws of the State of Wisconsin.

1. Emergency Authority of WEC and Governor

Even in the case of an emergency, qualified electors in Wisconsin still have legal rights that must be respected. The Wisconsin Elections Commission itself does not have the legal authority to delay or postpone any elections or elections-related deadlines. If the Commission wanted to adjust election deadlines due to an emergency situation or incident, it would have to seek a court order to affect any elections-related deadlines.

The Governor of Wisconsin has general emergency authority, and this authority has only been used sparingly and to accomplish immediate objectives in the past. In the event of a widespread and severe emergency, the Governor of Wisconsin could alter elections-related deadlines, but this authority would end shortly after the immediate emergency had passed. The Governor's office could initiate court action or request that the Wisconsin Department of Justice or the Wisconsin Elections Commission initiate court action to alter any deadlines.

2. Fusion Center (Incident Response)

a. Communication of Incident to Stakeholders

- i. Since the reports of elections-focused cyber threats from nation-state actors in 2016, the WEC has been working closely with the WSIC fusion center. The WSIC fusion center has members from the Department of Homeland Security, the FBI, the US Department of Justice, the Wisconsin Department of Justice, DOA's DET, the Wisconsin National Guard, and others. This collaboration provides authorized WEC staff with access to sensitive and classified materials, as well as weekly briefings on cyber threats in a wide range of industries.

b. Provision of Support to Elections

- i. In addition to intelligence, the WSIC has also provided enhanced monitoring and forensic capabilities. This has enabled the WEC to provide support to local elections officials that experience security incidents in a way that would not have been otherwise possible. For the November 2018 General Election, the WSIC was also able to provide logistical and materiel support, from communications officers to assist in monitoring social media to cyber response teams on standby to respond to incidents anywhere in the state.

c. Coordination with Wisconsin Emergency Management

- i. The WEC was able to take advantage of this infrastructure in November to provide local election officials with a 24/7 hotline for cyber security incidents. Had there been a security breach, election officials would have been able to immediately contact the WEM duty officer, who had instructions on how to contact appropriate cyber response teams and elections officials who would then work to mitigate the issue. This hotline was formed ad-hoc in the preparations for the election, but staff intends to formalize this or a similar hotline for future use.

3. WisVote Database Breach

a. Loss of Data Response Plan

Situation – **WisVote data has been lost due to disaster or malicious activity.**

Resolution – WEC staff will resolve the immediate cause as appropriate, and then restore backups. Currently, offsite backups have a Recovery Point Objective of not more than 24 hours.

b. Data Breach Response

Situation – WisVote data has been accessed by an unauthorized user.

Resolution – WEC staff will immediately lock the suspected account and investigate if there were any downloads or alterations of WisVote data. All WisVote users in that locality or office will change their passwords to prevent any additional data breaches.

The user of the compromised account that resulted in the breach will have their WisVote access reviewed by WEC staff and returned when it has been determined that they will be able to safely possess WisVote credentials.

c. Data Altered Response Plan

Sample Situation – WisVote data was altered due to an unauthorized user.

Resolution – WEC staff will work to immediately identify and lock suspected WisVote accounts. WEC staff will determine approximately when the data was altered and use available backup data to restore accurate data to WisVote.

4. State Law Enforcement – Department of Justice

WEC staff have met with representatives from the Wisconsin Department of Justice about Election Day preparations and potential lines of communication should an election security incident arise.

In the event that the WEC needs assistance from state law enforcement or the State of Wisconsin Department of Justice, the WEC Administrator will follow the internal emergency contact protocol established by WEC staff to quickly and effectively contact the appropriate resources at both agencies.

5. Internet Outage, MyVote Outage, WisVote Outage, or Server Event

The Wisconsin Elections Commission uses programs and applications that require an Internet connection and rely on technology maintained at the state level. In the event of a widespread Internet outage, election administration programs like MyVote, WisVote, and the official WEC website will be inaccessible, and response plans will have to be put in place.

a. Online Voter Registration

Sample Situation – MyVote is not accessible.

Resolution – While WEC staff works on re-establishing public access to MyVote, qualified electors can still register to vote with their municipal clerks in person,

on Election Day at their polling location, and by mail if the outage occurs at least 20 days before the next general or spring election. Voters should be directed to complete a paper voter registration and to provide a copy of a proof of residence document if necessary.

b. WisVote

Sample Situation – WisVote is not accessible.

Resolution – While WEC staff works on re-establishing access to WisVote and investigating the reasons why the WisVote system was not accessible, other WEC staff will communicate to credentialed users to resume their daily tasks if they can be temporarily transitioned to paper (processing voter registrations, accepting absentee ballot requests, etc.)

WEC staff will provide guidance on how local election officials should proceed with tasks that require WisVote access and will seek legal orders if needed to adjust any elections-related deadlines that could occur while WisVote access is restored.

6. Emergency Response Documents

In the event of an election security incident, every moment will count. It is vital that the Wisconsin Elections Commission have materials and clear protocols that are ready to be used immediately after an election security incident to quickly resolve the situation and return to normal agency business.

a. Contingency Plan for Agency

The Wisconsin Elections Commission has a contingency plan that details how the Wisconsin Elections Commission will be able to continue daily operations should normal daily operations be affected due to a security incident. Contingency plans detail the essential functions of the agency, delegation of authority, continuity facilitates to be used should the WEC offices be inaccessible, and how WEC staff will communicate these plans with other election partners and the public when appropriate.

Contingency plan details are maintained by administrative staff at the WEC and are periodically reviewed and updated.

Sample Situation – A security incident occurs at the WEC’s office and is no longer accessible.

Resolution – WEC staff will follow the most recent contingency plan procedures. WEC staff will also coordinate with other state agencies and resources to quickly resume daily operations safely in a secure location.

a. Emergency/Disaster Contingency Plan for Local Election Officials

The WEC has published a report detailing what local election officials should include in their contingency plans for the time surrounding, and on, Election Day. Topics to cover range from identifying what potential disasters could occur, reviewing what contingency processes from their county or municipality are already in place, and writing down the plan so that it can be easily followed by clerk staff in the event of an emergency.

If a local election official does not have an emergency/disaster contingency plan already in place, WEC staff will work with that local election official to begin the process of drafting a plan and offer up best practices in making an effective plan.

Contingency plan details are maintained by staff at the WEC and are periodically reviewed and updated.

Sample Situation – A local election official does not have an emergency/disaster contingency plan for their community

Resolution – WEC staff will provide the local election official with WEC-created emergency response templates and emergency/disaster contingency plan so the local election official can create their personalized plan.

WEC staff will also offer additional help in conducting an election security tabletop exercise that can help local election officials and partners understand the interconnectivity of different county and municipal government partners during a security incident.

E. County Level

While elections in Wisconsin are administered at the municipal level, County clerks play an important role. The 72 county clerks of Wisconsin serve as resources for municipal clerks and are responsible for providing certain election materials and training. County clerks are important partners in elections security as they are often the conduit for information from the WEC to Wisconsin's 1,852 municipal clerks. If you feel like you are experiencing an incident

that is not described in this report, please call the Wisconsin Elections Commission Help Desk at 608-261-2028, and your call will be routed to help resolve the situation.

1. WisVote

Sample Situation: WisVote appears to be working erratically.

Resolution: If only WisVote is experiencing issues, county clerk staff will call the Wisconsin Elections Commission's Help Desk. WEC staff will be able to troubleshoot the issue and see if it is an isolated event and the severity of the issue.

Sample Situation: WisVote credentials were compromised.

Resolution: County clerk staff will immediately contact the Wisconsin Elections Commission. It is vital to contact the Wisconsin Elections Commission in the moments after discovering that county clerk credentials may have been compromised. WEC staff will be able to lock your account to prevent any unauthorized access to private information, as well as provide guidance on how to regain access to a WisVote account with secure credentials.

In the chance that WisVote credentials have been compromised, county staff with WisVote credentials should immediately change their passwords to prevent any potential issues with their WisVote credentials becoming compromised in the future.

Sample Situation: The device that you use to access WisVote is malfunctioning.

Resolution: If possible, shut down the device and contact the county IT department/contact. If the device was not signed in to WisVote at the time of the issue, staff credentials may not be compromised, and the error may just be contained within the device itself.

If county clerk staff are concerned that county WisVote credentials were compromised, contact the Wisconsin Elections Commission immediately. WEC staff will be able to identify potential risks and preventatively lock certain county WisVote accounts to prevent any unauthorized access.

2. Voting Equipment

Sample Situation: The county clerk's office receives a call from a municipal clerk on Election Day that their voting equipment is not working.

Resolution: If possible, direct the municipal clerk to have election inspectors redirect voters to other voting equipment to continue the flow of voting while county clerk staff learn more about the situation. Voters are still able to deposit their ballots into the

auxiliary bin if necessary. Election Inspectors should also be instructed to explain to voters that their ballot will still be counted, and that the counting of ballots is a public process if voters want to ensure that ballots placed in the auxiliary bin are counted.

Contact the voting equipment vendor to see if the issue is something that can be repaired, or if the voting equipment vendor can conduct repairs. In addition to contacting the voting equipment vendor of the issue, county clerk staff should contact the Wisconsin Elections Commission Help Desk. This will allow state officials to be aware of the issue and provide any additional advice or resources.

Sample Situation: County clerk staff receive information that the voting equipment is malfunctioning at the municipal public test.

Resolution: Contact the voting equipment vendor and inquire whether the municipality's voting equipment issue is an isolated event. The voting equipment vendor will have the resources to address hardware issues that will need to be fixed before the voting equipment can be used in the polling location.

Contact the Wisconsin Elections Commission to alert them of the issue and provide them with timely updates.

3. Incident Response

Each county clerk's office should have an updated contingency plan and Election Day Emergency Response plans that outlines incident responses and parties to be contacted in case of an incident either before or on Election Day. The counties should also strongly encourage their municipalities to create similar plans. These plans contain sensitive information and should not be available to the general public.

In addition, counties should have a plan to aid municipalities should an incident require an escalated level of response and have the contact information to other county emergency and legal resources on-call on Election Day.

F. Municipal Level

Elections in Wisconsin are administered at the municipal level. Municipal clerks are tasked with preparing and administering elections for the various cities, towns, and villages around Wisconsin. While the WEC recognizes that municipal clerks across the state have different access to elections-related resources, they all still have a duty and responsibility to maintain the security of our elections. The Wisconsin Elections Commission serves as a statewide resource for all municipal clerks. If you feel like you are experiencing an incident that is not described in

this report, please call the Wisconsin Elections Commission Help Desk at 608-261-2028, and your call will be routed to a Specialist to better help resolve the situation.

1. WisVote

Sample Situation: WisVote appears to be working erratically.

Resolution: If only WisVote is experiencing issues, municipal staff will call the Wisconsin Elections Commission's Help Desk. WEC staff will be able to troubleshoot the issue and see if it is an isolated event.

Sample Situation: WisVote credentials were compromised.

Resolution: Immediately contact the Wisconsin Elections Commission. It is vital to contact the Wisconsin Elections Commission in the moments after discovering that municipal credentials may have been compromised. WEC staff will be able to lock certain municipal accounts to prevent any unauthorized access to private information, as well as provide guidance on how to regain access to WisVote accounts. While multifactor authentication helps deter WisVote access with stolen credentials, the user's password must be changed immediately.

In the chance that WisVote credentials have been compromised, have other municipal staff with WisVote credentials immediately change their passwords to prevent any potential issues with their WisVote credentials becoming compromised.

Sample Situation: The device that you use to access WisVote is malfunctioning.

Resolution: If possible, shut down the device and contact municipal IT department/contact. If the device was not signed in to WisVote at the time of the issue, staff credentials may not be compromised, and the error may just be contained within the device itself.

If staff are concerned that any municipal WisVote credentials were compromised, contact the Wisconsin Elections Commission immediately. WEC staff will be able to identify potential risks and preventatively lock municipal WisVote accounts to prevent any unauthorized access.

2. Voting Equipment

Sample Situation: Voting equipment is malfunctioning at the polling place.

Resolution: If possible, have election inspectors redirect voters to other voting equipment to continue the flow of voting while municipal staff learn more about the situation. If necessary, voters will still be able to deposit their ballots into the auxiliary

bin.

In a situation where there are supplementary pieces of voting equipment that were checked during the public test, these machines could quickly be deployed to the polling place. If there are no available backup voting equipment available, municipal staff should instruct election inspectors to have voters place their voted ballots in the auxiliary bin to be hand counted after the close of polls. Election Inspectors should also be instructed to explain to voters that all votes will be counted and that the counting of votes is a public process if voters want to ensure that ballots placed in the auxiliary bin are counted.

Sample Situation: Voting equipment is malfunctioning at the public test.

Resolution: Contact the voting equipment vendor and inquire whether the municipality's voting equipment issue is an isolated event. The voting equipment vendor will have the resources to address hardware issues that will need to be fixed before the voting equipment can be used in the polling location.

Contact the county clerk to see if there are any available machines that could be issued to the municipality for the upcoming election.

3. Incident Response

Each municipality should have an updated Election Day Emergency Response plan that outlines incident responses and parties to be contacted in case of an incident on Election Day. This response plan should be updated prior to every election and available at each polling location. Election inspectors will have training about their responsibilities as they relate to the plan, and an awareness of the physical location of the plan on Election Day.

G. Other User Levels

Wisconsin law refers to poll workers as election inspectors. Election inspector responsibilities regarding election security occur almost exclusively on Election Day. Inspectors are responsible for conducting elections at the polls on Election Day. This includes processing and securing voter registrations, ensuring only eligible voters receive a ballot, ensuring the process to receive a ballot is followed (photo ID, poll books, issuing voter numbers), ensuring each voter is at the correct polling place and receives the correct ballot, troubleshooting polling place issues, setting up and maintaining voting equipment, tallying ballots, and much more. If you feel like you are experiencing an incident that is not described in this report, please call the Wisconsin

Elections Commission Help Desk at 608-261-2028, and your call will be routed to a Specialist to better help resolve the situation.

1. Voting Equipment

Sample Situation – Voting equipment is malfunctioning.

Resolution - It is important to contact the municipal clerk right away if the voting equipment is malfunctioning to ensure that the equipment can be repaired or replaced as soon as possible. The municipal clerk will have the contact information for the county clerk, and potentially a representative from the company that supplied the voting equipment. Municipal staff will also know of any potential backup machines that could be sent to the polling place if the machine needed to be replaced entirely. The municipal clerk will serve as a resource in deciding what procedures to put into place should the Close of Polls procedures need to be adjusted.

If voters are still attempting to cast their ballots, instruct them to place their ballots in the auxiliary bin. When dealing with voting equipment errors on Election Day, it is vital to be transparent with voters and to inform them that their vote will still be counted. Wisconsin requires that every vote be cast on a paper ballot or on a machine with a voter-verified paper audit trail (VVPAT) that could be hand counted if need be. Voters can still fill out their paper ballot and place them in the auxiliary bin to either be later inserted into the voting equipment by the election inspectors, or to be hand counted if the voting equipment has not been properly fixed. All ballots that are properly completed will be counted, no matter if they are cast with the voting equipment or if they are hand counted after the polls have closed.

2. Electronic Poll Books

Sample Situation – There are issues with the Badger Book

Resolution – If the error occurs on Election Day, resort back to the paper poll book that was printed and provided by the municipal clerk to ensure that voters are processed in a timely fashion.

Contact the municipal clerk and have ready the serial number and labeled name of the problem equipment, a description of the specific nature of the issues, and roughly when the issue occurred. The municipal clerk will then contact the Wisconsin Elections Commission, and WEC staff will troubleshoot the issue over the phone.

H. Public Level

Voters, voter advocacy groups, and the media also play an important role in elections security. It is important for voters to understand the process and know what to expect when voting in Wisconsin. Therefore, it is the WEC's responsibility to partner with municipal clerks, voter advocacy groups, and the media to provide information to the public on elections security.

1. *Media*

Sample Situation - Voter encounters large amounts of misinformation about the voting process.

Resolution - Refer fellow voters to official WEC websites, publications, and voter outreach materials.

- i. The Wisconsin Elections Commission is the official agency tasked with enforcing and administering Wisconsin's election laws. Communications from the WEC via elections.wi.gov, myvote.wi.gov, verified social media accounts, and press releases sent from the WEC's administrator or public information officer are the official communication methods of the Commission. If you have questions on election information, call the Wisconsin Elections Commission at 1-866-VOTEWIS (1-866-868-3947) to be connected to WEC staff.