NOTICE OF OPEN MEETING

Wisconsin Elections Commission

Meeting of the Commission
Tuesday, August 13, 2019
9:00 A.M. Open Session Agenda

Wisconsin Elections Commission
212 East Washington Ave., Third Floor
Madison, Wisconsin

Commission to Appear by Teleconference

A. Call to Order

B. Administrator's Report of Appropriate Meeting Notice

C. Election Security Update

I. Manage Hardware Proposal for Local Officials
II. Public Information Campaign

Wisconsin Elections Commission

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

DATE: For the August 13, 2019 Commission Meeting

TO: Members, Wisconsin Elections Commission

FROM: Meagan Wolfe
Administrator, Wisconsin Elections Commission

Prepared and Presented by:
Tony Bridges, Election Security Lead

SUBJECT: Election Security- Managed Hardware Proposal

I. Background

Since 2016, the Wisconsin Elections Commission ("WEC" or "Commission") has devoted significant resources to strengthening the security of its core resources, particularly WisVote, the voter registration and election management system, and MyVote, the public voter information and online registration system. However, many of the systems vital to elections in Wisconsin are not under direct WEC control, such as local election officials' workstations. Election officials use these workstations not only to access vital voter and elections records in WisVote, but also to maintain their own records of voter data, print reports containing voter data, generate letters, print labels, send absentee ballots by email, correspond with voters, and perform many other tasks that are critical to running elections. Because each of these workstations access WisVote, the strength or weakness of any one workstation could affect the security of the entire state's elections infrastructure and the public's confidence in the integrity of the Wisconsin elections.

Local election officials do not have equal access to computer hardware, software, and support. Some have dedicated IT staff who are able to ensure the security of their workstations. Others work with contractors or perform their own IT maintenance. The quality of contracted IT support varies depending on the service provider and many do not have the resources to keep up with the constantly changing needs of IT security, including software patches and updates.

At present, the Commission's insight into the security posture of local election officials is limited. However, WEC staff knows that at least a handful of users are logging in to WisVote with outdated operating systems that are no longer receiving security updates, including Windows XP for which support ended in 2014. Additionally, hundreds of users are accessing WisVote with computers running Microsoft Windows 7. At present, Windows 7 is continuing to receive security updates. However, Microsoft has announced that it will stop providing free

updates for Windows 7 on January 14, 2020. After that time and until 2023, updates will be available for an escalating annual fee. Based on the end of support history with Windows XP, WEC staff can reasonably assume that a large percentage of users will neither upgrade before the deadline nor choose to pay for updates. Even those with current operating systems often fail to install current security patches.

The failure to maintain a current operating system exposes the user to tremendous risk. As an example, in March of 2019, Jackson County, Georgia systems were brought offline county-wide by a ransomware variant called Ryuk. Ryuk encrypted vital system components, including computers supporting emergency services such as 911 dispatch. Ryuk gained access to county computers through a vulnerability in a protocol used for file sharing in older networks. An update that fixed that vulnerability had been available since 2017 but was not implemented on the Jackson County systems. The county ultimately paid a ransom of $400,000, and still spent five weeks and dedicated significant resources to repairing damage from the attack.

A similar attack that impacted local election officials would pose numerous risks. It could, for example, expose confidential information, prevent the timely distribution of absentee ballots, prevent the timely printing of poll books, disrupt communications with voters, expose voters to potential cyberattack, destroy digital records, prevent the display of election night results, and dramatically impact voter confidence in the electoral process. The proposals described in this memorandum are designed to directly address these potential threats.

II. Proposal Overview

WEC staff recommends a three-part plan to address security risks created by elections processes running on thousands of independent systems. The intent of this plan is to assess the devices currently used to access WisVote, develop and provide guidance to effectively update non-compliant devices, and provide a managed loaner device to non-compliant users who otherwise lack the resources to obtain a comparable device.

First, the WEC staff will ascertain the existing security posture of these systems. The WEC can procure very specialized software that will enable visibility into the security posture of devices that connect to WisVote, including operating system patching, presence and effectiveness of anti-virus software, and the existence of known infections.

Second, WEC staff will identify points of weakness among users and develop specific recommendations to mitigate risks. Based on the results returned by this endpoint testing, WEC staff can provide tailored guidance to users explaining how to bring their systems into compliance with minimum security standards. WEC staff will work directly with users or with their IT departments to educate users and implement necessary changes.

Third, the WEC will create a loaner program to offer municipalities a way to rapidly achieve compliance for limited purposes over a limited period of time. The WEC will procure a limited number of low-cost devices that comply with Commission standards and can be easily managed and maintained from a central system owned by the WEC. If users are unable to bring their systems into compliance, and further certify that their governing bodies are unable or unwilling to procure replacement systems, the WEC may lend them compliant devices on a first-come-

first-served basis. The loaner program will include a sustainable support model to ensure hardware stays current and users have a place to seek assistance over the long term.

III. Endpoint Testing

The ability to remotely assess a user's security posture is essential to this program. Most users do not have the technical expertise to adequately assess their own systems. Furthermore, even if the WEC could physically inspect each clerk's computer, that inspection would only be valid for that day. Thus, a software-based system is the only way to independently and accurately capture the state of a user's hardware and software over time. With a software-based system, the WEC can perform security assessments at will and keep up with a constantly changing user base and evolving threats.

A handful of existing technologies are available that assess the security posture of a client computer requesting access to protected applications. The traditional mechanism for this is a system called Network Access Control (NAC) that is applied to Virtual Private Networks (VPN). A VPN is a cryptographic connection that is created over an untrusted network, such as the internet, to create a system where a more trusted network of computers can communicate as though they were directly connected to each other. The NAC portion of the process is responsible for ensuring that the endpoints of the network meet security policies before allowing the VPN to connect. It is probable that such a system could be made to meet the requirements of this program.

A traditional VPN is not ideal because it requires significant overhead in management and maintenance and requires an additional interface that is often confusing and unfriendly to end users. An alternative is to use a stand-alone NAC system without the VPN. Variations on this system are referred to by several names, such as Cloud NAC, web NAC, virtual NAC, or Software Defined Perimeter. In these systems, security policies similar to those available for VPNs are used, but instead of requiring the creation of a complicated VPN, are instead used as part of the authentication process for a web-based application. In this way, it is similar to the implementation of Multi-Factor Authentication, where we added a factor that is based on the security posture of the connecting device. This system could be made essentially invisible to end users.

Stand-alone NAC systems are all very similar. Agency staff would access management software and establish policies for security baselines based on industry best practices. Staff generally follows the Center for Internet Security baselines for security, which include items such as removing unnecessary communication protocols, maintaining complex passwords and monitoring for file changes. Users of the WisVote system would then be required to install a client on their devices. When the users attempted to access WisVote, the client would attest to WisVote that the device met the security policies before allowing it access to WisVote.

Based on market research, staff estimates this component will cost not more than $69,000 per year.

IV. Compliance Reporting and User Education

The WEC will aid users who fail to meet minimum security standards. With the Endpoint Testing tool described above, WEC staff can identify the biggest problems and develop specific recommendations to remediate shortcomings. Where appropriate, staff can likewise interact with local technical support providers – paid for by the locality – in order to help municipalities achieve compliance. If a user is unable to achieve compliance in a timely manner, staff may refer them to the loaner program described in the next section. Under exceptional circumstances – for example, the outright refusal to comply – the WEC could prevent a noncompliant user from accessing WisVote.

IV. Loaner Program

A. General Concept. There will inevitably be some number of election officials who lack the resources needed to achieve compliance quickly. Users unable to correct deficiencies expose WisVote, other users, voters and the election as a whole to increased risk. Assisting these users is critical to our collective security. Staff discussed these concerns with the Clerk Advisory Committee, particularly regarding concerns that assisting these users may be seen as unfair favoritism. The consensus of the committee was that the real inequity was that jurisdictions who are in compliance might be jeopardized by users who are not, and that any assistance that increases the overall security of elections was welcome. That said, staff is sensitive to the concern that providing support to the weakest link may be perceived as rewarding recalcitrance. To correct shortcomings without rewarding non-compliance, the WEC staff suggests a managed hardware loaner program designed to coax municipalities towards compliance.

B. Program Elements. For a WEC managed solution to appropriately fill this gap, it must meet several needs. It must be able to perform all the functions required by elections officials, or else they will find other ways to accomplish those tasks that may not meet security requirements. It must be centrally managed, or else without local IT support it will drift away from current security requirements or fail to adapt to future requirements. However, it should require minimal intervention from WEC staff in normal operation, or the agency's support capabilities will be quickly overwhelmed. And it must be cost effective, in order to assist as many clerks as possible for as long as possible. With those objectives in mind, WEC staff has developed guidelines for a program that would meet this need.

The hardware solution is the simplest component of the loaner program. Clerks inform us that their business processes can generally be broken into three subcategories: (1) browser-based applications such as WisVote; (2) office productivity applications such as Word; and (3) peripheral-device interface such as scanning barcodes or printing reports. Virtually any desktop or laptop currently available for purchase can handle these tasks. Procurement for these devices should therefore focus on ease of use and low cost.

Another essential part of the loaner program is the management process. There are several systems available today that allow for centralized management of devices, from updates and virus definitions to installed applications and desktop backgrounds. With centralized management, the WEC would set statewide policies that automatically propagate to every user of the managed devices, allowing for a high degree of security compliance with minimal staff effort.

Administration of a loan program is a significant challenge, and the WEC has neither the staffing nor the storage space to manage it. Instead, storage and transport of the devices and the management of the loan program should be handled by either the vendor providing the devices or a subcontractor. The WEC would purchase the rights to devices, but the vendor would retain those devices until a loan is agreed upon. Then the vendor would ship new devices from its stock to the loan recipients and handle the onboarding process. Loans would be granted free of charge on a first-come-first-serve basis to election officials who certify that they are unable to receive a compliant device through their governing body. The term of the loan would end on June 31 of the next odd numbered year, to provide the least possible disruption to election processes. As part of the procurement, staff will also investigate possible options for insuring the devices against loss or damage. The procurement should also provide a means for jurisdictions that wish to be a part of the managed program but have available funding to purchase devices from the vendor.

In addition to supporting municipalities unable to achieve compliance, the loaner program could also benefit municipalities that are targeted by malware. In a serious cyber incident, the state's Cyber Response Teams generally take all affected systems off the network immediately. Equipment is then analyzed by forensic experts before being wiped clean and re-imaged. These processes take time, leaving a municipality without hardware it may need to function – particularly if a municipality uses only one computer. If an event occurred immediately prior to an election, the effects could be significant. With a pool of compliant, secure hardware on-hand, the WEC could immediately lend hardware to an affected clerk and help sustain their operations.

C. Recommendation. Research conducted since the last Elections Commission meeting found 527 WisVote users with a PC or Apple Macintosh computer configuration that has reached end of life or will reach end of life in the next six months. These users represent our higher risk population and form the basis for our estimated requirements. Because a number of these high-risk users already have plans to update their systems, staff recommends an initial purchase of 250 devices, with an option to purchase 50 more if stocks are depleted before June 31, 2020. Based on market research, and including the services discussed in the next session over the lifetime of the devices, staff estimates this component will cost not more than $300,000.00.

VI. Managed Services and Technical Support

The final piece of this program is ongoing maintenance, replacement and technical support. Problems occur with all technology, and it is reasonable for borrowers to assume the WEC would handle those issues. However, providing day-to-day technical support for loaner devices could quickly overwhelm the WEC and staff would not be able to provide timely service around elections when it is needed most. Therefore, staff recommends including ongoing maintenance and support as part of the procurement for these devices, to include onboarding, offboarding, device-related technical support and training services. To reduce costs, a variable Service Level Agreement could be considered where the vendor would be obligated to respond quickly to requests near an election, but next business day during off periods.

Staff also requests authorization to create a new federally funded position to support the managed hardware program, anticipated Badger Book growth, and future security programs. To create federally funded positions, the WEC will need to submit an amended §16.54 request including a description of positions to be created using federal funds. The new position will

focus on implementing security best practices with agency technology including managed hardware, Badger Books, and other election security technological needs. WEC staff envisions this position working closely with the WEC Security Lead and IT Project Manager under the supervision of the Technology Director.

VII. Proposed Motions

WEC staff recommends the Commission approve the following actions:

MOTION #1: Direct staff to procure software, at a cost not to exceed $69,000, capable of monitoring end-user devices for security posture, to work with localities to achieve compliance with minimum security standards, and to conditionally prevent access to WisVote for noncompliance.

MOTION #2: Direct staff to develop a managed hardware loan program for users who are unable to achieve compliance. Authorize staff to request bids for 250 devices capable of meeting election official business needs that can be centrally managed by agency staff for security posture and application installation, including the administration of delivery, onboarding, offboarding, device technical support and training services. Total procurement and support costs combined shall not exceed $300,000.

MOTION #3: Direct staff to submit one additional §16.54 request to create a federally funded position and create position descriptions and determine appropriate classifications based on immediate security needs as well as future needs as identified through feedback collected from elections security partners, the cost of which is not to exceed $100,000 annually for the duration of the grant.

Wisconsin Elections Commission

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

DATE: For the August 13, 2019 Commission Meeting

TO: Members, Wisconsin Elections Commission

FROM: Meagan Wolfe
Administrator, Wisconsin Elections Commission

Prepared and/or Presented by:
Reid Magney, Public Information Officer

SUBJECT: Public Outreach Initiative

I. Introduction

This memo describes staff's efforts to advance the Commission's public outreach initiative to increase awareness and confidence in election security. It also contains staff recommendations for hiring an agency to conduct market research and assist the WEC and local election officials in communicating with the public about election security.

The Commission passed the following motion at its meeting on June 11, 2019:

> The Commission directs staff to seek proposals and award a contract for research and development of a public information campaign to educate the public about Wisconsin election security at a total cost not to exceed $260,000, which will be paid for out of the 2018 HAVA grant for election security. Following research and development of a campaign, staff will seek Commission approval for additional expenditures to implement the campaign.

Based on discussion at the meeting, staff interpreted the motion to mean the Commission wanted staff to identify and interview qualified vendors, and to recommend a successful vendor to begin the market research phase of the project, for approval at the special meeting on August 13.

II. Background

According to the U.S. Election Assistance Commission's (EAC) website which tracks and displays states' security planning efforts, multiple states have earmarked portions of their 2018 election security HAVA funds to conduct market research and to launch professionally created public information campaigns about election security. These states are planning to produce informative materials covering a range of topics including voting equipment security, recognizing misinformation, reiterating the importance of having an auditable paper ballot, and more. WEC staff, along with members of the Clerk

Advisory Committee on Security, believe that a professional public information campaign, rooted in initial and ongoing research about public perceptions, could effectively communicate election security measures in Wisconsin and help combat inaccurate or misleading information now and in the future. Staff and clerks also believe a campaign should be two-way, building in methods for the public to provide feedback about their concerns.

Both WEC staff and members of the clerk advisory committee expressed concerns about public perception of election security. Due to each individual state having its own election system, every state has implemented its own unique security initiatives. Explaining these unique security structures to voters in a resonate way can be difficult. When a reported security issue occurs in another state, voters may believe that it also affected Wisconsin's election system. To combat this, the WEC consulted with the Clerk Advisory Committee on Security to discuss the current issues they face concerning election security. Members shared that they have frequently presented the many different security measures that Wisconsin has in place that ensure a voter's ballot is counted how it was intended, but still noted an issue with combatting misunderstanding of election security in Wisconsin. Clerk members also identified a general lack of experience with working with the media as an issue specifically for clerks and their staff. WEC staff asked clerk members to discuss what could help Wisconsin voters become more aware of election security practices and efforts in Wisconsin. In particular, the clerks wanted the program to:

1. Highlight security measures already in place in Wisconsin, such as how voting equipment is secured, accuracy is verified, and the voter registration system is protected.

2. Dispel common misconceptions held by voters, especially highlighting ballot security and tallying.

3. Provide digital media options for social media and locality websites, without neglecting voters who do not use social media or frequent governmental websites.

4. Expand and rebrand the toll-free hotline the agency provides as part of its obligations under HAVA to include election security topics.

5. Include media training for clerks and their staff to better handle media inquiries and outreach.

Based on its discussions with other states and with local election officials, staff believes an important guiding principle for a successful approach in Wisconsin is connecting the market research and public information campaign by allowing the research to identify the methods and emphasis that should be used in a public information campaign, if any. While election officials nationwide have been focused on various potential risks and threats, it is important that any preconceived notions do not replace market research data in determining the best way to reach voters and the public with effective messages, or even determining to what extent a public information campaign is necessary.

III. Procurement

Due to the long lead time necessary to award a new state contract for services, Chief Administrative

Officer Sharrie Hauge worked with procurement staff at the Department of Administration (DOA) to identify existing state contracts the WEC could take advantage of, a process known as "piggybacking." DOA recommended that WEC make use of a relatively new state contract awarded by UW-Madison for "brand strategy, marketing services, web development, photography and videography services." Under the contract, more than a dozen approved vendors are available. Some vendors on the contract are full-service agencies while others are specialists in one area, such as social media or photography, and which may partner with other vendors to provide a fuller range of services.

Staff received permission from UW-Madison to piggyback on its contract. Under state procurement rules, WEC would be free to directly engage any of the qualified vendors on the UW-Madison contract. Staff identified five vendors on the contract who are full-service advertising agencies and would be able to provide WEC with market research services, as well as campaign development and crisis communications services if needed. Those five agencies were:

- Boelter & Lincoln, Milwaukee
- Creative Marketing Resources, Inc. (CMR), Milwaukee
- Hiebing, Madison
- KW2, Madison
- Vendi Advertising, La Crosse

Staff developed a Request for Information (RFI) document describing the services WEC is interested in procuring and posing a series of questions to the vendors about how they would approach the tasks. Those agencies were emailed a copy of the RFI on July 1, 2019. Hiebing and Vendi Advertising responded that they would not be submitting responses to the RFI. The remaining agencies had until July 10 to submit questions about the RFI to WEC staff, which were answered on July 11. Agencies had until July 15 to submit formal responses.

After reviewing the RFI responses from Boelter & Lincoln, CMR, and KW2, staff invited all three agencies to participate in half-hour interviews via conference calls, which were held on July 23 and 24. After evaluating the interviews, staff narrowed the field to Boelter & Lincoln and KW2, and invited those agencies to one-hour, in-person interviews on July 31 and August 1. Both agencies made excellent presentations.

Based on the presentations, interviews and experience, staff recommends the Commission engage KW2, which has a history of doing significant, outstanding work for the agency and its predecessor since 2011. KW2 conceived and executed the Bring It to the Ballot campaign to educate the public about the voter photo ID law starting in 2011. The firm also provided design and consulting services for the relaunch of the My Vote Wisconsin website in 2017. While the election security contract would differ in significant ways from those previous engagements, and while Boelter & Lincoln offered its own strengths, the consensus of WEC staff is that KW2 would be the best fit for this initiative.

IV. Scope of Work

1. Market Research

In response to the RFI, KW2 has developed a dynamic market research plan that combines qualitative (focus group) and quantitative (survey) research methods. The purpose is to help WEC understand what the public knows/believes about election security, where they get their information, and how election officials can best communicate with the public about this issue. That communication may be proactive, but it could also be in response to misinformation or disinformation about election security. It could also happen in the event of an actual cyber incident within our state or elsewhere that affects public confidence in election security.

KW2 recommends a three-step process:

1. Qualitative Key Informant Interviews

   KW2 will conduct several key informant interviews to frame the issues and our understanding of potential perceptions regarding election security around the state, and to further identify our hypotheses for testing. This step guides the survey tool and any directional changes they would recommend. For this step, they will conduct phone and in-person interviews with WEC leaders, local election officials, municipal and county clerks. This is not a quantitative study, so a representative size is not needed.

   After meeting with WEC staff, KW2 will prepare a discussion guide and conduct three to four key internal stakeholder meetings. During these interviews, they will be looking for directional information – a hypothesis on emotional and functional attributes – that will provide insight into the statewide quantitative research. KW2 will provide a discussion guide prior to these sessions, and a summary of findings upon completion of the research.

2. Statewide Quantitative Survey—Baseline and Optional Follow-up

   Using the directional data from the Key Informant Interviews KW2 will conduct a statewide survey to identify perceptions, issues and understanding around election security and integrity. This would provide WEC a roadmap showing who we need to communicate to, what their current baseline beliefs/perceptions of election security are and reveal their awareness of WEC, including perceptions of credibility concerning information conveyed by the agency.

3. Qualitative Focus Group Message Testing

   While KW2 is finishing the quantitative findings, it will develop messages that address any issues the research identifies. Message testing will determine what messages are most relevant to various audiences, whether or not they find them credible, and what type of action they would take after hearing the messages.

Primary market research and message testing would occur in September, October and November of 2019. Follow-up survey research could occur at multiple points during 2020, but most likely following the April 7 Spring Election and Presidential Preference Primary.

KW2 estimates the core market research would cost $183,300, broken down as follows:

- Key Informant Interviews, $12,000
- Statewide Focus Groups, $78,000
- Baseline Statewide Survey, $50,620
- Follow-up Statewide Survey, $42,680

Staff recommends budgeting up to $20,000 for additional market research to be used if new threats or unanticipated events appear to be altering the public's perceptions of election security and legitimacy. This would bring the total budget for market research to $203,300, which is below the $260,000 the Commission initially authorized for market research.

2. Communications Training and Response

Based on results of the market research, KW2 will develop communications training methods and materials for WEC and local election officials. These deliverables and costs will likely include:

- Media training sessions for election officials (three recorded webinars, one in-person session for WEC staff and five in-person sessions around the state for clerks), $38,000.
- Local Election Officials Toolkit, including traditional tools such as news release templates and social media resources, $35,000.
- 12 months of social and traditional media monitoring services, including a dashboard that will allow WEC staff to monitor the pulse of public conversation on election security, $30,000.
- Strategic and crisis communications consulting services as needed, $135/hour. At five hours per week for 52 weeks, that would total $35,100. The actual figure for this component would depend directly on election security events and developments and therefore this is only an estimate for planning purposes.

3. Campaign Development

Based on the market research, KW2 will develop recommendations for a dynamic public information campaign on election security, which staff will review and bring to the Commission for approval. Without having conducted the research yet, KW2 and WEC staff do not have an opinion about what specific methods and media should be included in a public information campaign. It could be as simple as WEC staff working with news media across the state to inform the public about how state and local election officials are working to ensure the security and integrity of elections. It could involve using existing, unpaid social media channels (Facebook, Twitter, etc.) to spread the word. It could also involve producing informative videos, creating paid social media ads and banners, producing public service announcements for broadcast and online media. Whatever the campaign is, it will need to be dynamic and adaptable in the event that new threats appear or shifts in public opinion occur during the election year.

Based on our experience with the voter photo ID public information campaign, KW2 and WEC staff are very aware of the challenges and costs involved in running an ad-based campaign during a presidential election year when many candidates and political organizations will conduct extensive advertising campaigns. KW2 demonstrated and provided examples of "non-traditional" public information campaigns that they had conducted in the past, which may be appropriate for the Commission to consider based on the results of the market research.

WEC staff and KW2 recommend including any campaign development services in a subsequent agreement after the results of the market research are evaluated. Therefore, no costs for campaign development are included in this summary.

IV. Recommended Motion

WEC staff recommends the Commission approve the following action:

MOTION: The Commission directs staff to engage the KW2 agency, using the existing state contract with UW-Madison, to conduct market research regarding election security and to develop training and communications tools to support state and local election officials as they communicate with voters and media about election security. Also based on the research, KW2 will develop proposals for a public information campaign to educate the public about Wisconsin election security, which will be subject to further approval by the Commission. The cost of the initial research, election official communication training, and campaign proposal development will not exceed $341,400, and will be paid for from the 2018 HAVA grant for election security.