WISCONSIN ELECTIONS COMMISSION

212 EAST WASHINGTON AVENUE, 3RD FLOOR
POST OFFICE BOX 7984
MADISON, WI 53707-7984
(608) 261-2028
ELECTIONS@WI.GOV
ELECTIONS.WI.GOV

INTERIM ADMINISTRATOR MEAGAN WOLFE

COMMISSIONERS

BEVERLY R. GILL
JULIE M. GLANCEY
ANN S. JACOBS
JODI JENSEN
DEAN KNUDSON
MARK L. THOMSEN, CHAIR

MEMORANDUM

DATE: For the May 24, 2018 Commission Meeting

TO: Members, Wisconsin Elections Commission

FROM: Meagan Wolfe
Interim Administrator, Wisconsin Elections Commission

Prepared and Presented by:

Tony Bridges	Riley Willman
WisVote Specialist	Election Administration Specialist

SUBJECT: Elections Security Staff Update

I. Introduction

In March 2018, the Wisconsin Elections Commission (WEC) received a $6,798,318 grant award to improve the administration of elections for Federal office, which includes technology enhancements and election security improvements to its systems, equipment, and processes used in federal elections. State law requires compliance with the §16.54 process for a state agency to accept federal funds and this process involves several steps. An initial step was completed when the agency received written confirmation from the Department of Administration with approval for the acceptance of the grant money on April 24, 2018.

II. Request for Six Federally-Funded Positions

The Wisconsin Elections Commission granted staff authority to explore and make purchases regarding security-related software and request the creation of six federally-funded positions at its April 18, 2018 meeting (at a cost not to exceed $600,000 annually). Position authority may be granted through the §16.54 process and the hiring of the six project program positions will allow the WEC to implement and achieve the grant's goals and objectives, and to comply with the terms and conditions of this grant.

The Wisconsin Elections Commission requested the creation of 6.0 full-time equivalent 48-month federal project positions from the Department of Administration (DOA) on May 9, 2018. A draft position description for each position was submitted for consideration as part of the agency's request. If approved, these positions would be federally funded from June 1, 2018 – June 1, 2022. The six requested positions are as follows:

1. Information Technology Project Manager
2. Elections Security Trainer
3. Elections Data Specialist
4. Information Services Technical Services Professional
5. Voting Systems Specialist
6. Grants Accountant

Staff awaits approval of the positions from DOA, and will work to fill the positions in advance of the 2018 fall election cycle if that approval is granted. Once the position authority has been granted, agency management plans to circulate the draft position descriptions and a proposed strategy for incorporating and utilizing new staff for comment and input by commission members and existing staff.

III. Technical Implementations

In addition to the ongoing support that the WEC provides local election officials, staff is also pursuing several different options to improve technical controls that secure access to WisVote and other critical systems. These are combinations of software and hardware that make it more difficult for malicious or simply careless actions to jeopardize the safety of WEC systems and data. The Commission approved the agency incurring expenditures regarding these technical upgrades at its meeting on April 18, 2018 and staff has provided updates on these projects below.

A. Multi-Factor Authentication

Multi-Factor Authentication (MFA) is an important technology in preventing malicious access to user accounts. Proper implementation of MFA can prevent an attacker from gaining access to a user account, even after they have stolen the user’s password. The WEC is working to implement MFA as a log-in requirement for WisVote as a means to safeguard the large number of accounts with access to the system. However, the large number of users and lack of central control over those users, as well as the way in which WEC systems integrate with DET systems, present unique technical and logistical challenges for implementation. WEC staff are in discussions with DET to determine the best and most expedient way to implement MFA. DET has assigned WEC a project manager to assist with the implementation of this protocol. They have proposed a solution, but DET does not believe it can be implemented in time for the August Partisan Primary but does believe a solution can be implemented prior to the November General Election. Staff is pursuing that option, while researching short-term alternatives that can be used for the August Partisan Primary.

B. Active Directory Federated Services

The WEC uses an industry-standard authentication technology called Active Directory to manage user accounts and passwords that allow access to WisVote. Active Directory works seamlessly within a network for server access, but to provide access to a website like WisVote, it requires an intermediary service called Active Directory Federated Service (AD FS). Currently, WisVote uses an AD FS server operated by DET. This setup allowed WisVote to launch in accordance with the 2016 deployment schedule, and currently relieves WEC of some development and maintenance requirements. However, it also ties the authentication of WisVote users to the authentication of several other State of Wisconsin systems. This configuration makes it harder for WEC developers to make any changes to the log-in process for WisVote. WEC staff is investigating the development of a standalone WEC AD FS server which would allow the agency to more readily customize many details of the log-in process from branding to permitted encryption ciphers, and may also simplify MFA implementation and the tracking and maintenance of user agreements. A server request for this project has already been submitted to DET and system testing is planned to determine how challenging the proposed customizations will be.

C. Clerk Emails

DET manages the email systems for state employees, including all WEC staff. DET employs a number of security controls on those emails, including Cisco Email Security (commonly referred to by its former name of Ironport), which protect users from malicious emails. DET blocks hundreds of thousands of malicious emails each day using this system so that they never reach the end user, and therefore are never able to compromise any systems or users. The majority of clerks, however, do not have this level of protection on their email systems. WEC staff and DET are working on providing a solution that would enable all users of the WisVote system to have an email address that is routed through these security systems, dramatically reducing the risk to clerks and the WisVote system from social engineering and malware. Conversations with DET and clerks on this topic are in the initial stages, and both sides are enthusiastic about this move. Staff expects to communicate options to clerks soon.

D. Centralization of Web Applications

The WEC provides access to several web applications for clerks and for the general public. Several of these systems have previously been designated as high-security systems and are maintained within the state network on virtual servers provided by DET. This setup affords them a high degree of initial security, including strong perimeter security, protection against bandwidth attacks (DDOS), top-tier endpoint security, third-party penetration testing, and more. However, some sites that had not previously been designated high security have been hosted by a third-party vendor. Based on a number of factors, including a reassessment of the impact of malicious modification of those sites, WEC staff has decided that those sites should be hosted on the state network as well. This change will require a significant amount of coordination with the current service provider to avoid disruptions during the transition, and staff expects to complete the transition this fall.

E. Vulnerability Scanning

Agency servers exposed to the internet are regularly scanned by the Department of Homeland Security for known vulnerabilities, and servers within the state network are regularly scanned by DET. However, DHS does not do internal scanning, and DET does not currently provide the agency with comprehensive reports regarding the results of scanning efforts. Staff has made arrangements with DET to increase the scope and accuracy of the internal scans, and to provide reports on the results directly to WEC staff for review. The first trial of this scan is expected to be complete by May 24.

IV. Local Election Official Security Training and Communications Update

Staff is currently in the planning stages of implementing a new and robust election security training program to be rolled out in June 2018. These trainings and materials are being implemented in conjunction with the security training material being prepared by staff for the WisVote Learning Center, as well as agency technological initiatives.

A. Local Election Official Security Training

In March of 2018, Wisconsin Elections Commission 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 Boston, Massachusetts. 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 can occur leading up to Election Day.

The purpose of a TTX is 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 on Election Day. These incidents are scripted before being introduced into the simulation and cover a wide variety of topics and severity, ranging from weather-related issues that could potentially impact polling places, to larger cybersecurity incidents that would require working with IT professionals. Throughout the TTX, participants can test their continuity plans against the incident injects in a low-stress environment to determine their efficacy. In addition to creating and improving continuity plans, a goal of the TTX is for participants to see how they can successfully implement measures to prevent election security incidents from occurring.

WEC staff saw value in participating in an election security TTX, and concluded that Wisconsin county and municipal election officials would benefit from both the training and simulation exercise. WEC staff has created an elections-security train-the-trainer program in partnership with Wisconsin county clerks to reach as many of the 1,853 municipal clerks as possible. 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 the materials and staffing resources provided by the WEC. WEC staff has created eight regions throughout the state and has organized a training and TTX opportunity in each region starting in June. This schedule was designed to ensure that all county clerks could attend a regional training and have adequate time to conduct a training of their own with the municipal clerks in their county and region.

WEC staff is conducting a training and TTX event in Madison on May 31 with county clerks from 17 different counties from across the state. After these clerks have participated in the TTX, WEC staff has asked for the participants to help facilitate the trainings occurring in their region for county clerks who did not attend the training and TTX event in Madison. This approach will additionally allow for the facilitating clerks to get experience leading an elections security TTX. WEC staff will also work with the county clerks on how to improve the training and materials to make the regional training as effective as possible. WEC Staff has five regional trainings currently scheduled for June and is working on scheduling additional events ahead of the fall election cycle.

B. Communications Plan

Maintaining communication with key election security officials and the public during an election security incident presents many challenges. Frequently, incident details evolve as more information is learned, and it is vital that local election officials keep key officials and the public updated on developments. WEC staff understands that time is of the essence when handling an election security incident, and is developing a plan to assist local election officials in communicating effectively and quickly in the event of a potential incident.

WEC staff will prepare communication materials and contingency plan templates that will be useful to clerks throughout the election administration process. Feedback from the recent election security survey that was sent to county clerks indicated that clerks have found WEC-produced templates and step-by-step guides helpful and efficient resources. A security communications template and guide will be created by WEC staff that allows for the local election officials to quickly outline the appropriate contact information for resources in the event of a potential security question or incident. The goal of these guides and templates are to help local election officials have a high-level understanding of best practices when communicating during an incident, as well as to reinforce that WEC staff are a resource for clerks to contact if they have questions or need assistance in resolving an incident.

C. Monitoring and Distributing Security Alert Information

WEC staff has been partaking in cyber defense webinars from the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC). These organizations have been identified as a key cyber security resource by the Department of Homeland Security for their ability to bring together election security officials from various states. The updates and information that comes from the MS-ISAC and EI-ISAC webinars assume a large knowledge about information technology and cybersecurity practices. WEC staff has made the decision that the MS-ISAC and EI-ISAC updates will be monitored by staff who will then send pertinent information to the local election officials to ensure that information is getting to all involved officials in a timely and productive manner.

V. <u>Collecting Feedback from Key Election Security Partners</u>

As WEC staff works on implementing security trainings and publishing guides for local election officials before the August and November elections, there are additional plans to implement a second phase to keep Wisconsin's elections safe and secure. WEC staff is currently in the process of creating an avenue for key election security partners such as DHS, DET, county clerks, municipal clerks, and members of the public to provide feedback on how the HAVA security funds should be spent.

Municipal and county clerks in Wisconsin have differing access to in-office security and IT resources, and WEC staff will solicit feedback from the local election officials on how to best provide election security assistance. Keeping Wisconsin elections secure will require high levels of collaboration between WEC staff and key election security partners to ensure needs are being met.

In March, WEC staff sent a survey to county clerks to ask for information about their current election security programs before planning a statewide training program. A similar approach will occur after the

WEC staff conducts regional security trainings and tabletop exercises around the state to improve training and to maximize the effectiveness of future elections security communications and events. Feedback will be solicited after every training event so that participants can provide local election official perspective on the WEC-led training programs. Additionally, ideas and input will be solicited from local election officials and key election security partners unable to attend WEC-led trainings on how they believe the WEC can effectively use the HAVA security funds.

To keep local election officials involved in future election security developments, WEC staff plans on inviting county clerks to collaboratively review and provide suggested edits to election security publications to ensure the materials are as useful as possible to a variety of local election officials. Once feedback is received, WEC staff will disperse the security publications for all clerks so that they can work to prevent a security incident from occurring, and understand quick and clear next-steps to take in the event of a potential security incident.