WISCONSIN DEPARTMENT OF
ADMINISTRATION

SCOTT WALKER
GOVERNOR
SCOTT A. NEITZEL
SECRETARY
Division of Enterprise Technology
Post Office Box 7844
Madison, WI 53707-7844
Voice (608) 267-0627
Fax (608) 267-0626

Date: September 26, 2017

To: Michael Haas, Administrator, Wisconsin Elections Commission

From: David Cagigal, State of Wisconsin Chief Information Officer

Subject: Division of Enterprise Technology Security Efforts

Background:

On Friday, the Elections Commission was notified that Internet-facing election infrastructure in Wisconsin was unsuccessfully targeted by "Russian government cyber actors." According to the Department of Homeland Security (DHS), the actors scanned internet-connected election infrastructure likely seeking vulnerabilities, but the attempt was unsuccessful in Wisconsin.

Michael Haas of the Elections Commission is seeking more specific information, including when the scanning activity occurred in 2016.

The following is being provided at the request of the Elections Commission to summarize the actions taken to secure state systems in advance of the 2016 elections.

Conclusion:

The Division of Enterprise Technology worked closely with the Elections Commission to proactively protect our data and systems. Wisconsin did not experience a cyber incident or breach. As DHS confirmed last Friday, any attempt to target the states election data was unsuccessful and no data was compromised or lost.

Definitions:

Event: An observable occurrence in an information system or network. An event sometimes provides an indication that an incident is occurring or at least raise the suspicion that an incident may be occurring. For the State of Wisconsin, these are examples of events for one year:

- 1.2 Billion Filtered Emails
- 9 Million Vulnerability Scans
- 40,000 Potential Malware Downloads
- 42,000 Attempts to Exploit Web Applications
- 505,000 Attempts to Break Passwords

Incident: An occurrence that actually or potentially results in adverse consequences to (adverse effects on) (poses a threat to) an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.

Breach: Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected information.

Timeline:

8/18/2015 DET performed a Vulnerability Assessment of Elections systems in preparation for the November 2016 election. A multitude of critical vulnerabilities were identified and recommendations for upgrades were provided to Elections staff.

01/11/2016 Based upon DET recommendations, Elections upgraded and implemented new versions of Elections systems to remediate all vulnerabilities identified in the 2015 assessment, including updates to prevent Structured Query Language (SQL) injection (SQLi) which was identified in the Illinois incident.

6 to 7/2016 Media reports of hacking:

- State of Illinois
- State of Arizona

8/1/2016 Multi State-Information Sharing and Analysis Center (MS-ISAC) Advisory received related to election systems including information about activities occurring in other states.

- The SQLi vulnerability exploited in Illinois did not occur in Wisconsin because of the upgrades implemented in January 2016.
- DET blocked the malicious IPs identified in the advisory.
- DET reviews all the advisories recommendations and confirms that they have been addressed.

Note: We generally receive dozens of MS-ISAC alerts in any given month.
We routinely block IP addresses based on advisories and/or observed events.

8/15/2016 DHS Secretary Johnson holds a conference call with state election officials nationwide to warn of danger and offer assistance.

8/24/2016 DET reviews the 8/18 FBI Flash with Elections and confirms that the malicious IPs identified have been blocked.

Planning begins for DET to perform Vulnerability Assessment of the new Elections systems.

9/13/2016 Elections Commission staff hosted a joint meeting with the Federal Bureau of Investigation, the U.S. Department of Justice, the Wisconsin Department of Justice, Wisconsin Emergency Management and representatives of the Milwaukee and Dane County District Attorney offices

to discuss election day preparedness and to designate emergency points of contacts in their respective offices for emergencies that may occur on Election Day.

9/13/2016 DET performed an updated Vulnerability Assessment (external and internal) of Elections systems.

9/22/2016 Department Homeland Security performed a Vulnerability Assessment (external) of Elections systems.

9/28/2016 DET meeting with Elections to review Vulnerability Assessment Report findings.

9/30/2016 DET implemented rules to block foreign IPs from accessing the My Vote system in the User Acceptance Test environment.

10/3/2016 DET implemented rules to block foreign IPs from accessing the My Vote system in the Production environment.

10/6/2016 DET received notification from the MS-ISAC Security Operations Center (SOC) of Suspicious Traffic from a Known Malicious IP Related to Voter and Election Compromises.

- DET investigated the log information provided and the activity occurred on 7/30 and 7/31/2016. The traffic attempted to access a nonexistent server at the Department of Workforce Development network. There was no attempt to exfiltrate data since there were only two inbound web site access attempts that received no response as there was no server at the requested address.

- The suspicious IP address was listed in the MS-ISAC Advisory received on 8/1 and was blocked on 8/2/2016. The scan had no effect on any state system and no data was exfiltrated.

- Elections had previously been notified on 8/24 that this IP address was blocked.

10/7/2016 DET began monitoring Elections' systems every 2 hours. All states received a notification to remain vigilant in the final month leading up to the election.

10/10/2016 DET provides security awareness materials for Elections Commission to utilize in communications to the Local Clerks.

10/12/2016 Question from Elections regarding scanning events. DET provides data for scanning events specific to Elections January 1, 2016 to date. None of the scanning events resulted in an incident or data breach. Note that the average daily scanning events of all State of Wisconsin systems is 25,000 per day. Elections systems activity was consistent with the rest of the enterprise.

10/14/2016 DHS requested that DET share information related to IP addresses identified by the August 18 FBI Flash alert.

DET reported events involving 4 of the 8 addresses. None of the events generated an incident or vulnerability to Wisconsin's system.

Summary of events:

- One outgoing, or internal computer initiated request, to access a malicious website. This is commonly occurs in conjunction with an internet advertising pop-up or banner. This attempt was blocked by our web content filtering tool and no data was exfiltrated (8/29/2016). This blocked content request came on an elections commission network, likely a desktop computer.

- Two emails were dropped and not delivered by email filtering (1/7/2016 and 7/26/2016). These emails went to various addresses at the Department of Health Services, Department of Corrections, and the Department of Agriculture, Trade, and Consumer Protection.

- Two inbound web site access attempts that received no response since there was no server at the requested address (7/30 and 7/31/2016). These events were related to the Department of Workforce Development.

- One visit to www. JobCenterofWisconsin. com. No data was exfiltrated.

10/14/2016 DET received an updated FBI Flash distributed via MS-ISAC, NASED and direct from FBI.

11/8/2016 DET provides hourly monitoring of Elections' systems for Election Day. No incidents reported.