



STATE OF MICHIGAN
JOCELYN BENSON, SECRETARY OF STATE
DEPARTMENT OF STATE
LANSING

MEMORANDUM

Date: July 10, 2023
To: Municipal and County Election Officials
From: Jonathan Brater, Director of Elections
Subject: Security of Qualified Voter File and Electronic Pollbooks

Introduction

Election officials have experienced a series of attempts to access election materials that, if disclosed, pose privacy threats to Michigan voters and security threats to Michigan's election system. At times, these attempts have been accompanied by aggressive and even threatening language and behavior. Consistent with the Michigan Election Law and its responsibility to safeguard election security in Michigan, the Bureau of Elections (the Bureau) has instructed clerks that while Qualified Voter File (QVF) and Electronic Pollbook (EPB) records are public and subject to disclosure, certain components of these systems cannot be released without compromising voter privacy and election system security.

This memorandum provides further explanation of these issues and information for clerks to consider when reviewing public records requests with their legal counsel. It also describes the potential consequences of providing inappropriate access to election equipment to unauthorized individuals. Additionally, the memorandum addresses several false claims that have been made about QVF and EPB data and election administration in Michigan.

Record Requests Seeking QVF and EPB Data

Clerks have received requests for access to QVF and EPB data in a variety of different formats, including:

- Requests under the Michigan Freedom of Information Act (FOIA)
- Demands that records be preserved for "investigation"
- Demands to perform "inspections" of election records or equipment

Regardless of the format of any request to inspect QVF or EPB data, clerks should consult with their own counsel for legal questions regarding any of these requests.¹ The Bureau provides the following information in this memorandum: a summary of applicable provisions of FOIA and the Michigan Election Law; a description of the manner in which the Bureau has responded to

¹ Any clerk who receives a subpoena, request to preserve records pursuant to a lawsuit, or a request to inspect records from law enforcement should consult with legal counsel and inform the Bureau of Elections and the Michigan Department of Attorney General.

specific requests, and; instructions not to disclose certain materials that pose a threat to election system security if released.

Requests for Electronic EPB Files

Clerks have received requests for electronic copies of EPB materials in various formats. These include requests for “an electronic copy of the Qualified Voter File (QVF) extract”; an “electronic pollbook flash drive”, a “CSV- Comma separate value format”, or other similar requests. At times, these requests have been accompanied by “helpful” instructions showing clerks how to potentially compromise the security of their election systems and render their election equipment unusable by illegally providing security-compromising information to unauthorized individuals.

Before responding to these or any FOIA requests, clerks should consult with their legal counsel regarding the requests and exemptions that may apply. Under FOIA, officials may shield sensitive information from disclosure. In the case of EPB files, the Bureau of Elections instructs clerks that they must not publicly release data or files that would reveal the software design or data architecture of the EPB. The Bureau gives this lawful instruction² under its supervisory authority pursuant to MCL 168.21, 168.31, and 168.32, as doing so could compromise the Bureau’s ability to secure and safeguard the software and data from hacking, theft, loss or destruction, and accordingly interfere with the Bureau’s obligation under the Michigan Election law to provide EPB software to clerks. MCL 168.668b.

In response to previous FOIA requests regarding EPB data, the Bureau of Elections has not disclosed these records because the records sought constitute “cybersecurity plans, assessments, or vulnerabilities” that are exempt from disclosure. The Bureau has an interest in maximizing the protection and defense of its information systems, which outweighs the public interest in the disclosure of this information as the release of this sensitive information could jeopardize the security of Michigan’s electoral process. MCL 15.243(1)(y). In addition, the responsive records include proprietary software information, security feature information, and sensitive information which, if released, “would disclose a person’s cybersecurity plans or cybersecurity-related practices, procedures, methods, results, organizational information system infrastructure, hardware, or software.” MCL 15.243(1)(z). Additionally, these files contain sensitive information regarding jurisdictions’ EPB laptop(s) that might compromise the security of these laptops.

EPB files also contain personal identifying information such as full birth dates for voters, which are exempt from disclosure. MCL 168.509gg. Attempted manual redaction of personal identifying information may not be sufficient to protect this information from disclosure if the software and program files are disclosed.

² See MCL 168.931(h) (“A person shall not willfully fail to perform a duty imposed upon that person by this act, or disobey a lawful instruction or order of the secretary of state as chief state election officer[.]”)

If clerks receive a FOIA request for EPB data, the requestor can be directed to the county clerk for paper pollbook copies or to the Bureau for the log file or voter history.

Notwithstanding the above restrictions on the release of certain information, there are numerous ways in which members of the public can review public QVF and EPB data. Clerks can provide the paper records they are legally obligated to maintain for the required retention period after each election, as soon as the security period has elapsed. Certain specific data derived from the QVF and EPB is subject to disclosure under FOIA, including the lists of registered voters from the QVF and the paper printout of the EPB generated on election night.

If members of the public are interested in verifying the names of individuals registered to vote on a certain date or included in the EPB, they may obtain this information by submitting a FOIA request for publicly available records. If members of the public with concerns about EPB data wish to verify the names of individuals who cast ballots, they can also do so by submitting a FOIA request and reviewing the paper applications to vote completed by all in-person voters and the absent voter ballot applications submitted by all absentee voters.

Electronic records such as the EPB log file or voter history can be requested from the Bureau. Requests for EPB data must be directed to the Bureau to ensure that sensitive information related to both individual voters and the EPB are removed before public disclosure of otherwise available information. Even if clerks were to attempt to redact a voter's date of birth and other personally identifiable information, the disclosure of security and technical information is also exempt from FOIA and may not be properly redacted if produced by clerks, instead of the Bureau.

Demands to Disregard Lawful Instructions from the Bureau of Elections

Clerks have also received communications demanding that they disregard instructions contained in the Bureau of Elections communications, including the Recount/Release of Security Memorandum circulated after each election. The Bureau's instructions are lawful directives in compliance with state and federal law.

Going back to at least 2012 (under Secretary of State Ruth Johnson), the Bureau has issued a directive to destroy electronic copies of the EPB and flash drive. As clerks are no doubt aware, numerous candidates of both major political parties have won statewide elections since 2012. This procedure is necessary to safeguard security and voter privacy. Clerks destroy electronic copies only after they have already printed the paper copy of pollbook information (which must be retained for the required retention period).

Clerks must comply with this instruction regardless of whatever claims private individuals make. A private individual has no authority to instruct clerks on their duties. Whatever "investigation" these individuals claim to be conducting or threats of "prosecution" they may make toward local or state officials, in the absence of a court-issued subpoena or other court order, clerks are not required to comply with their demands. If clerks do receive one of these demands, they should consult with their attorney on how to respond.

Clerks should also be wary of private individuals, including self-proclaimed “experts,” attempting to instruct them on the issue of whether disclosure of electronic materials would or would not constitute a security concern. In reality, it is often not possible for an individual unfamiliar with a system to determine whether any one individual piece of information, if known, would be useful in compromising that system. This is one of the reasons software and data elements which may, on their own or in combination with other elements, jeopardize security are not disclosed. Similarly, clerks should not accept at face value claims from private individuals, whatever expertise they claim to have, that clerks can easily redact security-related or personal identifying information.

Consequences of Improper Disclosure

Clerks should understand that the disclosure of this sensitive information may compromise the integrity of Michigan’s elections and may warrant an investigation by the Department of State, Department of Attorney General, or Michigan State Police. Improper disclosure may also result in fiscal implications for the jurisdiction. Specifically, disclosure could require the purchase of new EPB laptops for each precinct for which data was compromised.

False and Misleading Claims About QVF and EPB Data

Individuals seeking improper access to QVF and EPB records have made numerous false or misleading claims about QVF and EPB data and election administration in Michigan. Although making or believing false statements has no bearing on whether individuals are permitted to access a record, clerks may find these explanations useful in communicating with the public or other local and county officials, including law enforcement.

Election Turnout and Voter History

Some individuals have claimed that because, in past elections, the total number of ballots tabulated statewide does not exactly match the number of voters with a voter history indicator in QVF, this means that election results and files cannot be trusted, or that there is some sort of unknown or unexplained irregularity involving voter data.

In reality, these numbers do not match exactly because they come from two different sources. County-certified election results are based on the number of ballots cast and tabulated in each jurisdiction, as determined by the county canvass. This includes canvasser review of tabulator tapes showing election night results, in addition to any corrections or adjustments at the county canvass and recounts, if applicable.

Voter history in QVF is based on entry of voter history data from the EPBs (for in-person voters) and absent voter ballot return envelopes (for absentee voters). Following each election, each clerk uploads their EPB data for each of their precincts to the QVF. This automatically updates the voter history in QVF for all voters recorded in the EPB as voting at the polling place. Alternatively, clerks can manually add voter history to the QVF using the paper printout of the EPB.

If any of Michigan’s 1,520 municipal clerks do not update QVF with EPB data for any of their precincts, voter history for voters in those precincts will not appear in QVF even though those voters did in fact appear at the precinct, apply to vote, get recorded in the poll book, and cast

ballots. Following each election, the Bureau sends multiple communications and reminders to clerks to add voter history data to the QVF. Most clerks do so promptly, but some are delayed and some fail to do so.

This was the case in the November 2020 election, as it was in other past elections. Approximately 5.57 million ballots were cast in the November 2020 election according to certified results. As of April 2021, when the Office of the Auditor General reviewed QVF data for its audit of the Bureau, voter history for approximately 5.53 million voters had been uploaded to the QVF. In subsequent months, the Bureau sent additional communications to clerks reminding them to add voter history data to the QVF, and more clerks did so. As of 2022, the number of voters showing history in QVF for the November 2020 election was approximately 5.55 million.

Ultimately, a small percentage of jurisdictions did not add QVF data for at least one of their precincts in 2020 which meant that a small percentage of voter history was not recorded in QVF. Approximately 99.6% of voter history was uploaded in the QVF for the November 2020 election, which is a higher percentage than was uploaded for the November 2016 election (approximately 99.0%) and November 2018 election (approximately 98.5%). In subsequent elections, the percentage of voter history uploaded has increased even further.

EPB Time and Date Records

Individuals have claimed that the absence of a specific “time stamp” on some voter history tables is suspicious because, on election day, the EPB records the specific time at which a voter appeared on Election Day. These individuals misunderstand the table they are viewing. In reality, some QVF tables include “00:00” in the time field because the record is referring to an election *date*, not a *time* on election day. Elections occur all day, so it does not make sense for QVF to display any specific time. Like other programs that include voluminous amounts of data, QVF generates tables of data that are programmed and populated using numerous databases.³ When there is no entry needed for a field (for example, a time field corresponding to election day), the default value that databases display is “00:00.”

Voter History from Previous Addresses

Some voters who have moved from one jurisdiction to another in Michigan have noticed that voter history from prior elections, when they voted at their prior address, may appear as voter history from their current address. This is because the old version of QVF (QVF Legacy) did not track the jurisdiction where a past vote occurred. One of the many benefits of QVF Refresh, released in 2019, is that voter history from prior addresses can be tracked at the prior address. Therefore, voters who moved to and voted from prior addresses in elections that occurred after QVF Refresh was released will see voter history appear as having voted at the prior address.

³ Some individuals have claimed that there are multiple QVF “databases” and that this is somehow being used to perpetuate fraud. Aside from being impossible for the reasons described later in the memo, this claim is based on misconceptions regarding the QVF. The QVF is not a single “database” but instead a program used by the Bureau and Clerks for many purposes, requiring numerous tables and reports, which are in turn programmed and populated by numerous databases. For an explanation of what a database actually is, see this explanation from Microsoft: <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-are-databases/>.

However, votes that occurred at addresses when the voter's move predated QVF Refresh will display at the current address. This is not because of some nefarious purpose, but because QVF Legacy did not have the data capability as the current system.

QVF Record Identifying and Voter ID Numbers

Some individuals have claimed that the fact that there are multiple identifying numbers corresponding to voter records in QVF is suspicious. In reality, there are multiple numbers for security reasons. Voters have a public voter ID number in QVF and the EPB, which is public and disclosed in public record requests. QVF also contains separate record-identifying numbers that correspond to voter records, which are used for security and verification purposes (and which are not publicly disclosed for security reasons). Again, the non-disclosed record-identifying number is not different from the voter ID number for some nefarious purpose, but as an internal verification and security measure.

Security Procedures Used to Verify EPB is Offline

As clerks are aware, the EPB used on Election Day must be offline and laptops operating the EPB software must be turned to "airplane mode" to ensure there is no internet connection. In order to make sure that EPBs are offline, the EPB software is designed to receive a periodic "Ping" from the State of Michigan network on Election Day to check for improper internet connectivity. If the Ping detects an internet connection on the EPB laptop, the EPB software displays a warning message instructing the user to disconnect the laptop from an internet connection by turning the laptop to airplane mode. Some individuals have suggested this connection is suspicious, when in fact it is a security feature designed to ensure EPB laptops remain offline throughout Election Day.

General QVF-Related Conspiracy Theories

In general, some individuals have pointed to various data or program elements in QVF and claimed – whether because QVF data is imperfect or incomplete, because these individuals do not understand what they are looking at, or some combination of the above – that this shows some broad conspiracy to perpetrate election fraud. While it is of course true that QVF – a constantly changing voter file that needs to be updated whenever a voter registers, moves, cancels a registration, dies, applies for an absentee ballot, or various other activities – will never be 100 percent accurate or up to date, this does not mean there is some conspiracy to manipulate QVF data to perpetrate fraud. In fact, in recent years the Bureau and clerks have done more than ever before to keep QVF accurate and up to date.⁴

Regardless of how accurate or up to date QVF is at any given time, however, the suggestion that QVF could be used to perpetuate massive undetected election fraud is without merit. Even if one were to assume that Bureau staff (many of whom have worked at the nonpartisan Bureau of Elections for years or decades under multiple Secretaries of State of both political parties) and staff at the nonpartisan Department of Technology, Management, and Budget were involved in such a scheme, it would require thousands of clerks and election inspectors of both political parties to be involved as well.

⁴ For more information on how QVF is kept up to date, see <https://www.michigan.gov/sos/elections/voting/voters/voter-registration-cancellation-procedures>.

This is because while QVF is used to maintain *electronic* registration and voting records, voting is done by human beings using *paper* ballots, in elections that are run by municipal clerks across the state. In addition to the paper ballots, there are also polling place applications to vote (which must be completed by in-person voters, and which are retained by clerks after election) and absentee ballot applications (which must be completed by absentee voters, and which are also retained by clerks after elections). These materials provide an independent, *paper* record of all the individuals who cast ballots in an election. If there were actually some kind of fraud being perpetrated using QVF, this could be easily proven by reviewing these paper records.

In many respects, these nonsensical claims about QVF are similar to the false claims previously made about ballot tabulation equipment, which if true could have been proven by reviewing paper ballots (when in fact, reviews of paper ballots all confirmed that tabulators counted ballots accurately).

Additional Information and Support Available

It is unfortunate that election officials continue to be subjected to false claims, abusive behavior, and even threats. Whatever assertions individuals make about election officials, clerks should be mindful that there are legal avenues for individuals to pursue these assertions. If individuals disagree with a FOIA determination by a local or state official, they can file a lawsuit. If they believe criminal activity occurred, they can make a complaint in writing to law enforcement.

The Bureau encourages election officials to communicate with local and state law enforcement regarding any threats they may have received, and to continue to communicate with law enforcement regarding the various false claims and allegations of criminal activity that some individuals continue to make. Clerks are also encouraged to communicate with municipal and county government associations for additional independent support and advice. Finally, the Bureau of Elections remains available for any additional questions you have or support you may need. If clerks believe that any unauthorized or unsupervised access to their equipment may have occurred, they should contact the Bureau immediately. Please do not hesitate to contact the Bureau if we can be of further assistance.