Director's Message on Cybersecurity

As I'm sure you're all aware by now, one of the major points of interest for this General Election is cybersecurity. Specifically, members of the public want to know the steps we're taking to ensure our election systems are secure, votes are not tampered with, and the integrity of the vote is protected.

First off, it is important to note the following:

1. We use paper ballots so we have a hard copy backup of the results we report on Election Night.

2. After each election, we conduct an audit by hand of a sample of the ballots and compare it to our reported results. This practice helps us find any discrepancy between our reported results and the actual votes as a result of a cyber-attack on our equipment or tabulation system.

3. Our tabulation systems and voting equipment are not connected to the internet nor are they connected to any other networks.

4. We have bipartisan balance amongst all 85 CCBOE employees. No single person can access a ballot vault. This requires two individuals, one R and one D, each of whom have a passcode. In order to enter, the system requires both the R passcode and the D passcode.

These four practices have been in place for many elections, and are a major reason why we are yet to experience a critical cybersecurity breach. In many ways, they already put us ahead of the game with cybersecurity. However, there is still more that can be done to further bolster our security systems.

It is no secret that election tampering is a credible threat in today's society. In response to this, the Federal Government provided $380 million to states for cybersecurity funds (Ohio has received $12 million of this sum). As a result, the Ohio Secretary of State has made improvements to its IT infrastructure and updated the statewide voter registration database with additional security features. The SOS has also held various cybersecurity themed training sessions across the state, which were attended by CCBOE and County IT employees.

Another requirement from the Secretary of State is for BOEs to create an Elections Infrastructure Security Assessment. We are partnering with a private cybersecurity consultant who will put our systems through a variety of tests, making note of which areas need the most improvement. We will then be able to directly troubleshoot those areas.

With all of these practices, we're confident that we've significantly reduced our vulnerability to a cyber-attack. However, this doesn't mean we can ease up on our vigilance when looking out

for such an attack. If you should ever come across any suspicious activity, it is important you immediately notify us by calling (216) 443-8683.