Frank LaRose
Ohio Secretary of State

DIRECTIVE 2019-07
May 6, 2019

To: All County Boards of Elections
Directors, Deputy Directors, and Board Members

Re: Reporting of Security Events

SUMMARY

Over the last several years, the Secretary of State's Office, the bipartisan boards of elections in each of the 88 counties, and our law enforcement and first-responder partners at the local, state, and federal levels have worked diligently to enhance the already strong security posture around Ohio's election infrastructure. Despite this community's vigilance, "security events" (a broad term that can encompass everything from a pulled fire alarm at a school, a vehicular accident that takes out an electric pole and electricity to a polling place, to severe weather events, and more) can still occur.

The purpose of this Directive is to define the types of "security events" that must be reported to the Secretary of State's Office and to provide a streamlined reporting mechanism for doing so.

Additionally, the Secretary of State's Office would like to identify a Technical Point of Contact ("TPOC") for each board of elections. Boards of elections that contract for external IT support services provided either by the county or a third party are required to share this Directive with the boards' TPOC. Please send each boards' TPOC contact information to [redacted].

INSTRUCTIONS

A. Reporting

In the event of a security event in your county during the early voting period and continuing through Election Day, you must immediately notify the Secretary of State's Office. In order to stream-line the reporting of any security events, you must use the following email to relay the relevant information: [redacted] If you are unable to relay the information via email, you must contact the [redacted]. Even if local law enforcement or other first responders are aware of your security event, it is the responsibility of the local election officials to report the nature of the event to our office using this email address.

TLP: WHITE
UNCLASSIFIED//FOR OFFICIAL USE ONLY

B. Types of Events

The following is a list of possible "security events" that must be reported to our office; this list is not exhaustive. If you do not know whether an event is required to be reported, it is best to report it.

1. Unauthorized entry or attempt to gain unauthorized access to storage facilities, polling places, early vote centers, and/or offices of the board of elections (regardless of whether on private or public property that is used by the board of elections).

2. Incidences of phishing,[1] including spear-phishing,[2] or attempts to hack county voter registration systems or websites, to include similar efforts against seemingly unrelated county government entities.

3. Attempts to access, alter, or destroy systems used to qualify candidates; produce and deliver ballots; procure, manage and prepare voting equipment; process request for absentee ballots; and store and manage administration process and procedure documentation.

4. Unauthorized access or attempt to access, or unexplained inaccessibility or unavailability of, IT infrastructure or systems used to manage elections, including systems that count, audit, or display election results on election night and systems used to certify and validate post-election results.

5. Attempts to hack, phish, or compromise personal or professional e-mail accounts and social media accounts of elections officials, staff, and precinct election officials.

6. Hacking attempts or successful hacks into political party or candidate headquarters or IT systems, including e-mail.

7. Attempts to access, hack, alter, or disrupt infrastructure to receive and process absentee ballots through tabulations centers, web portals, e-mail, fax machines; attempts to interfere with votes sent through the U.S. Postal Service.

[1] *Phishing* is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

[2] *Spear-phishing* is the fraudulent practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information.

8. Compromises of any networks and/or systems, including hardware and/or software, to include tactics, techniques, procedures and impact observed on election-related networks and systems; evidence of interference detected on county networks or systems for cyber security indicators of compromise.

9. Attempts to persuade an elections official to engage in illegal activity or deviate from established practices in an effort to impact the administration of the election.

10. Instances of any unexplained disruption at a polling place or training locations for precinct election officials, including early voting locations, which block or inhibit voter participation. Disruptions may include social media posts or robo-calls or texts reporting closed or changed polling places, or physical incidents at polling places, including distribution of false information.

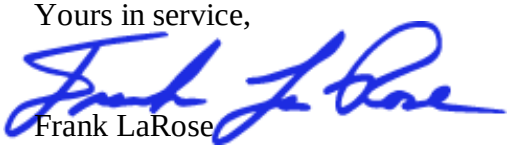
11. Disinformation efforts to alter or shutdown government web sites to foment social unrest or alter voter participation (including via social media or other electronic means).

12. Unauthorized entry of centralized vote counting/tabulation locations or electronic systems or networks used by board of elections to count voted ballots.

13. Impacts to critical infrastructure that limit access to polling places or information from elections officials, such as power, natural gas, water, internet, telephone (including cellular), and transportation (including traffic controls) outages.

If you have any questions, please contact the [redacted].

Yours in service,



Frank LaRose
Ohio Secretary of State

TLP: WHITE
UNCLASSIFIED//FOR OFFICIAL USE ONLY