CAMBRIDGE GLOBAL ADVISORS

MEMORANDUM

TO: WYOMING LIBERTY GROUP
FROM: CAMBRIDGE GLOBAL ADVISORS
SUBJECT: ELECTION SECURITY THREATS & EXPLOITS
DATE: AUGUST 12, 2020

Coming out of our discussion on August 6th, Cambridge Global Advisors (CGA) was tasked with developing a "dystopian list" of the various threat scenarios that exist for the exploitation of our voting systems and processes to inform Wyoming Liberty Group's messaging on this topic. Since 2016, significant cybersecurity weaknesses in our election ecosystem have been exposed. On top of this, it is anticipated that additional difficulties will arise as a result of COVID-19-related election administration workforce shortfalls and voting infrastructure malfunctions. Such problems would cause irregularities in collecting and counting absentee and other remotely-cast ballots, as well as long lines at polling stations.

The following list outlines the most common ways in which our country's election security may be compromised and recommendations for how to approach them.

Ransomware Attacks on Voter Registration Databases

With a ransomware attack, hackers restrict election officials from accessing their own data and demand large sums of money before restoring access, or refuse to comply altogether. The risk of this occurring requires properly backing up these databases so records of absentee ballot requests, ballots that had been mailed to voters, and returned and counted ballots are not lost. With this in mind, daily backups of the voter registration and absentee ballot data must be kept on separate machines that operate in separate systems. While this will not prevent a ransomware attack, it will mitigate the damage. In the event that a system becomes inoperable, officials can switch to another, which should be no more than a day behind in data updates.

Attacks on Election Websites

Attacks on government election websites, such as distributed denial of service (DDoS) attacks or SQL injections, can delay or change the results published to the website. Hackers are also capable of spreading false information about a locality's voting procedures and/or requirements by creating fake election websites. To counteract this threat, election officials should compare raw election data to the matching website data to ensure the correct results are being publicly reported.

Technical Failure or Hacks of e-Poll Books or Touch Screen Voting Machines

Electronic poll books and touch screen voting machines are at risk of being affected by intentional malware or unintentional technical flaws. In the event of such challenges, in-person voters could face hours-long delays. To prepare for and overcome these malfunctions, election officials should use backup paper records and make multiple paper-based poll books accessible to the polling place. Polling stations should also have enough paper ballots to allow most voters in the precinct to vote with real, not provisional, ballots that are counted that day in case voting machines malfunction.

Localized Disinformation

Disinformation continues to pose a major challenge, especially in the midst of the COVID-19 pandemic, which has provided bad actors with an array of new subject matter and messaging tactics to promulgate. Officials should deliberately track instances of disinformation and devise mitigation plans that include:

- Working with social media platforms to remove posts and accounts
- Assessing trends of disinformation
- Anticipating specific erroneous claims in the lead-up to Election Day
- Preparing strategies to counteract claims of election fraud and any other reason to disqualify the results