Microsoft

Defending Democracy Program

The 2020 U.S. Elections: Readying for the Challenges

BACKGROUND

When the Defending Democracy Program was founded in the spring of 2018, the threat to democratic institutions from nation-state adversaries seemed clear. Election officials around the world are now dealing with a new challenge to our democratic institutions—a global pandemic. The emergence of COVID-19 during a presidential election year in the United States potentially threatens access to the polls at a critical time. As election officials look for ways to take action to ensure voters' access is not disrupted, they should also use this opportunity to address the security challenges that have been in the forefront of the public's consciousness since 2016. At Microsoft, we believe that defending democracy includes ensuring that democracy continues to function at its most fundamental level.

PANDEMIC CONTINGENCY MEASURES TO HELP FACILITATE ELECTIONS

There is a growing chorus of election officials, media pundits, concerned citizens and academics[1] calling for swift action by Congress, key federal agencies and state election bodies to work together to address barriers and innovate in order to ensure secure and accessible elections for all in 2020. Microsoft believes two actions in particular, if undertaken swiftly and decisively, will contribute to a smooth election this November:

Increase access to absentee voting

Enable a curbside or portable voting solution

[1] "How to Protect the 2020 Vote from the Coronavirus", https://www.brennancenter.org/our-work/policy-solutions/how-protect-2020-vote-coronavirus

Increase Access to Absentee Ballots

The awareness of vote by mail has grown in the past several weeks as states have acted quickly to support their upcoming primary elections in the midst of increasing concerns about the spread of COVID-19. Voting by mail is deployed differently depending on each state's laws and procedures. In most states, the more common way to describe a voter returning their ballot by mail is the term "absentee voting".

When it comes to contingency planning for the upcoming general election, it would be a significant challenge for states who do not typically accept large numbers of ballots by mail to switch to entirely vote by mail. In states where vote by mail is already the norm, such as Oregon and Washington, the necessary infrastructure, budgets and even culture already exist. It would be difficult for other states to replicate that in a handful of months, especially under current remote working conditions[2]. There are some tangible steps that states can take, however, to expand existing absentee voting processes so as to provide a safe method of voting for all in November:

ENABLE NO EXCUSE ABSENTEE VOTING

Currently one third of states[3] require a voter to submit an excuse to justify not voting in person. Several states have already begun waiving this requirement for their primaries, which is encouraging. Even if done as an emergency measure specifically for 2020, extending this relief to voters in all states for the general election would be a huge step in the right direction, reducing the burden on states and removing the barriers to increased voter participation.

ENABLE ONLINE ABSENTEE BALLOT REQUESTS

Ideally, in an emergency effort such as this, states would be able to automatically generate absentee ballots for all registered voters and mail them directly. However, the cost and infrastructure to enable that effort is likely out of reach for many states this close to the general election, even with the additional funding provided by the CARES Act. As an alternative, states should provide voters an option to go online to request an absentee ballot, versus requiring a request to be made in person at a local election official's office or by mail. This efficient method of requesting an absentee ballot is currently only available in ten states[4]. Those states can serve as models for others looking to expand their options.

MAKE ABSENTEE BALLOT PROCESSING EASIER

In some states, regulations do not allow poll workers to begin processing absentee ballots until the day of the election; additionally, in four states poll workers even have to wait until the polls have closed before counting can begin.[5] This is manageable in an election where the vast majority of votes occur in person; however, as the states encourage more voters to mail their ballot in, election authorities need to develop additional capacity to handle processes related to these votes, such as signature verification. Enabling poll workers to start processing ballots before election day ensures faster results and a more efficient process.

[2] "Rapidly Scaling Up Absentee Voting in an Emergency", Matt Blaze, https://www.mattblaze.org/papers/Emergencyvoting.pdf

[3] "In two-thirds of the states, any qualified voter may vote absentee without offering an excuse, and in one-third of the states, an excuse is required." https://www.ncsl.org/research/elections-and-campaigns/absentee-and-early-voting.aspx

[4] Ten states have an online portal that permits voters to request an absentee/mailed ballot: Delaware, D.C., Florida, Louisiana, Maine, Maryland, Minnesota, Oklahoma, Pennsylvania, Vermont and Virginia. https://www.ncsl.org/research/elections-and-campaigns/absentee-and-early-voting.aspx

[5] Four states do not permit the processing of absentee/mailed ballots until after the polls close on Election Day https://www.ncsl.org/research/elections-and-campaigns/absentee-and-early-voting.aspx

Enable Curbside or Portable Voting Stations

Some states may not be able to scale an enhanced absentee voting process in time for the general election, and even those who do may have some voters who prefer voting in-person. Given that gathering to vote at a polling place could potentially still pose challenges come November, states should consider what alternatives they can make available to the public to be offered alongside expanded vote by mail.

One emerging approach is to deploy portable voting stations, either set up curbside at the normal polling place, or contained in a vehicle that can relocate to alternative voting locations. Some states already allow curbside voting for voters with disabilities, but it is not commonly built to scale for a larger population.

Exactly what form a portable voting system takes will depend heavily on the voting locality and their current system of voting. For example, for a system to be truly portable, it would likely need the pollbooks, which are used to verify a voter's eligibility to vote, to also be electronic rather than only printed binders. This way, once a voter casts his or her ballot at one mobile polling station, all poll workers' books will be updated to show he or she has cast their ballot and cannot vote again at another location. The fundamentals of such a system already exist, though this could be an opportunity for enhanced security by incorporating newer technologies, such as end-to-end verifiability (described in more detail below).

To implement curbside or portable voting options by November, states must move to identify and remove any regulatory, equipment or capacity hurdles needed to ensure a successful model.

CYBERSECURITY THREATS FACING U.S. ELECTIONS

While COVID-19 is a new and unexpected threat to U.S. elections, it is certainly not the only one. Challenges of nation-state interference and concerns around the security of election systems were already at the forefront of many officials' minds.

That said, election security has made significant progress since 2016. State and local election officials have spent countless hours in cybersecurity trainings hosted by technology companies, universities, and civil society groups. The U.S. Congress has authorized over $800m in the past two years to fund vital election security workloads at the state and local level. The CARES Act provides an additional $400m that states can use at their discretion to expand mail-in and early voting and online voter registration, as well as help secure in-person voting sites in response to the impact of COVID-19 on the election process. Increasingly, points of contact are being established between key stakeholders in government and the private sector to share best practices on improving security that can be applied to the upcoming general election. These are all positive steps in the right direction and should be acknowledged as a marked improvement. However, the race to securing democratic elections does not have a finish line, and much remains to be done.

Even before the emergence of the global COVID-19 pandemic, election systems in the U.S. faced an outsized threat in the form of nation-state adversaries. Microsoft's Threat Intelligence Center (MSTIC) has focused on tracking nation-state cybersecurity threat actors for more than a decade. Over the past year, most of the nation-state cyber activity targeting political campaigns and think tanks tracked by the MSTIC team has originated from actors in four countries: Iran, North Korea, China, and Russia. In 2016, attacks against NGOs and academia, which often involve spear-phishing against individuals at those organizations, served as a precursor to direct attacks on political campaigns. The adversaries behind these attacks have a stated goal of seeking to diminish voter confidence in the processes that are at the very core of our democracy. We should anticipate that we will see more attacks on campaigns and election processes in 2020 in furtherance of this goal.

Another point of concern is that of ransomware attacks on both voter registration and election systems. Ransomware attacks encrypt key datasets and thus render them inaccessible unless the victim pays a "ransom" hoping for restored access (which is by no means certain). While no election system has yet to be targeted in such a way, there have been similar attacks against other parts of state and local government systems, including in Atlanta (GA), Baltimore (MD), Cleveland (OH), Greenville (NC), and more than 20 communities in Texas. It is reasonable to expect that there exists a credible threat of a ransomware attack on an election system com November.

These threats against our election systems could get further exacerbated by adversaries attempting to exploit uncertainties around the COVID-19 pandemic.There have already been reports about an increase in cybersecurity attacks against other critical infrastructures including healthcare providers and NGOs, using COVID-19 themed phishing-lures[6].

[6] "Protecting Against Coronavirus Themed Phishing Attacks", https://www.microsoft.com/security/blog/2020/03/20/protecting-against-coronavirus-themed-phishing-attacks/

Election Security Policy Measures

Given that these threats show no sign of relenting, stakeholders in government and private sector alike must continue to seek innovative solutions. Many of the problem areas Microsoft has addressed since the inception of the Defending Democracy Program have focused on the technological needs of the election community. While technological solutions are a key component of addressing the threat of election interference, much can be done by way of advancing sound securitypolicies. Therefore, in addition to the urgent actions necessitated by the COVID-19 pandemic, Microsoft also advocates that the following changes be implemented to further improve the security of elections in the United States:

- Require paper trails
- Require post-election audits
- Apply end-to-end verifiability (E2EV)
- Provide consistent funding for state and local election officials
- Apply a multi-stakeholder approach to countering foreign interference

REQUIRE PAPER TRAILS

There is a deficit of trust[7] between voters, the technology with which they engage in the voting process, and those that build and administer these technologies. While we do not advocate that the federal government prescribe the specific method by which a vote is cast, there is broad consensus on one aspect of voting — that **there should be a voter-verified paper trail of the ballot**.

This does not mean that paper must always be the method by which a vote is cast. There are numerous emerging technology solutions — such as Microsoft's ElectionGuard technology described above — which include ballot marking devices or scanners that work in concert with paper while also enabling state of the art security.

Regardless of how the paper record is created during the voting process, ensuring a paper trail will provide voters with a level of confidence that there is a physical artifact that reflects their intended vote, and perhaps most importantly, it will enable another crucial aspect of securing elections: post-election audits.

REQUIRE POST-ELECTION AUDITS

Any robust security strategy includes layers of secure systems and processes. If one process fails, another layer exists to ensure the integrity of the overall system. Elections are no different. One process that has near-universal support from the security and election communities is that of a **post-election audit**.

Post-election audits can take a variety of forms and be executed in many ways. In the U.S., there has been recent growth in the testing of a specific kind of post-election audit called a "Risk Limiting Audit", or an RLA. RLAs require manually checking a statistical sample of paper ballots to see if the official election results, which are typically recorded electronically, match. Microsoft applauds advocates of this method and concur that, when conditions allow, **RLAs are the preferred method to statistically determine election integrity while preserving individual voter privacy.**

Regardless of which type of post-election audit is deployed, this added effort greatly increases the likelihood that an anomaly or mistake is detected and in turn ensures a reliable result that voters can trust.

[7] "Trust, Facts and Democracy," Key Findings, Pew Research Center, July 22, 2019- https://www.pewresearch.org/fact-tank/2019/07/22/key-findings-about-americans-declining-trust-in-government-and-each-other/

APPLY END TO END VERIFIABILITY

End-to-end-verifiability (E2EV) is a cutting-edge approach to election security that enables voters and members of the public to audit the integrity of an election[8]. E2EV seeks to achieve three primary objectives: 1) enable voters to verify that their vote was properly cast; 2) enable voters to ensure that their ballot was included in the final tally; and, 3) allow anyone — the public, media, candidates, etc. — to confirm that the official tally of the election was accurately reported.

This can be achieved by encrypting the ballot, whether cast on a ballot marking device or a hand-marked paper ballot scanned into the system. The voter receives a verification tracker that enables them to confirm online at the end of the election that their ballot was counted. At that time the public is able to run the complete encrypted results through a verifier, where — without decrypting the ballots – they can confirm the accuracy of the published election results.

E2EV therefore creates an election where any anomaly or intrusion will be detected. The encryption itself is a strong security measure, but the true strength is the ability to *know* if anything has been tampered with, thereby instilling confidence in the voters and creating a disincentive for adversaries. And the benefit to voters is the ability to confirm that one's vote was actually counted.

E2EV offers a best practice for increasing election security, and we believe policymakers should support efforts aimed at deploying it in voting processes. Microsoft has embraced this technology and created the first open-source, free and commercially viable E2EV solution called ElectionGuard. Interested parties can access this free software via its GitHub repository[8], or they can reach out to their election vendor for more information about how they plan to integrate ElectionGuard in their product offerings. Microsoft, in partnership with VotingWorks and the Wisconsin Election Commission, recently conducted our first ElectionGuard pilot in an election in Fulton, Wisconsin[9]. It was a complete success. For more information or to learn more about this effort, please contact the Defending Democracy Program at Microsoft at protect2020@microsoft.com.

PROVIDE CONSISTENT FUNDING FOR STATE AND LOCAL ELECTION OFFICIALS

State and local election officials need increased and consistent federal funding to consistently refresh to the most secure technology. While periodic infusions of cash, such as those released by congress in 2018 and 2019 along with the funds recently made available by the CARES Act, are undoubtedly beneficial, they place election authorities in a difficult position. If they choose to spend these funds on voting machines, as many have, they do not know if they will have the funds in the future to cover maintenance on those machines, including security updates. Our adversaries are agile and will move quickly to find security vulnerabilities. Ensuring cybersecurity is a never-ending function that requires predictable and reliable funding. If election officials had the ability to budget three or four years into the future, they could ensure they are deploying the most secure technology at all times.

As beneficial as newer machines and reliable maintenance is, states would benefit greatly from additional personnel. With a reliable stream of funds dedicated to securing a state's infrastructure, a state may be able to dedicate a full-time resource as a CISO or Cybersecurity Director — common in the private sector — who could in turn drive a long-term vision and policy to ensure the security of the state's election systems. Butadding a salaried employee is a difficult choice to make when subsequent, long-term funds are unclear.

[8] ElectionGuard GitHub Repository- https://github.com/ElectionGuard

[9] "Microsoft hopes this technology can help fix America's elections" - https://www.cnn.com/videos/business/2020/02/22/microsoft-electionguard-voting-security-orig.cnn/video/playlists/stories-worth-watching/

APPLY A MULTISTAKEHOLDER APPROACH TO COUNTERING FOREIGN ELECTION INTERFERENCE

Countering attempts at foreign interference in democratic processes and institutions will require a coordinated, long-term effort that is supported by governments, private sector actors, civil society, academia, and of course, voters themselves. One notable initiative in this context is the Paris Call for Trust and Security in Cyber Space[10] which Microsoft supports. One key principle endorsed by the Paris Call is Principle #3: *Strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities.*

To date, the Call has so far been signed by over 1000 stakeholders from industry, civil society and academia as well as over 75 governments and 29 local governments and public authorities. In the U.S., to date Colorado State, the Commonwealth of Virginia and Washington State have endorsed the Paris Call along with numerous U.S. cities and municipalities. Microsoft is one of the private sector signatories and **we encourage other state and municipal governments to endorse the Paris Call** which has become the single largest cybersecurity declaration globally.

Moreover, the Paris Call has provided a platform for signatories to come together in various "communities of action" to further advocate for and help implement these principles. Microsoft has partnered with the Alliance for Securing Democracy to lead a community of action focused on "Countering Foreign Election Interference" and we encourage other interested stakeholders to join this effort.

CONCLUSION

Ensuring additional methods of voting are available in times of a global pandemic and improving the security and trustworthiness of elections cannot be solved by the public or private sector acting alone. In a time where unprecedented public health challenges, as well as sophisticated nation-state actors have the potential to disrupt elections, all stakeholders must work together in new ways to protect our core democratic processes. Microsoft stands ready to do its part and we look forward to working with election officials, policymakers, our customers and our partners to advance these proposed solutions.

If you would like to learn more, please contact our
Defending Democracy Program at
protect2020@microsoft.com

[10] The Paris Call for Trust and Security in Cyberspace, https://pariscall.international/en/