MATT BLAZE [1]

RAPIDLY SCALING UP ABSENTEE VOTING IN AN EMERGENCY

10 MARCH 2020 - DRAFT

This is a brief (and by its nature, incomplete) summary of infrastructural and technological challenges for large-scale emergency voting in US civil elections, focused on the likely scenario that might arise if COVID-19 infections reach pandemic proportions and cause disruption to normal election infrastructure. For our purposes, we assume that:

- Existing regimes of in-person voting at local precincts might have to be sharply curtailed or eliminated in some or all jurisdictions for health and safety reasons. Decisions might not be made until a only short time prior to the general election.
- A possibly significant fraction of the electorate will be confined to their homes and unable to travel.
- A possibly significant fraction of the electorate will be confined to some other location, possibly outside their home jurisdiction, and unable to travel.
- Basic infrastructure – power, water, telecommunications, postal service, etc. – will largely continue to function, possibly at degraded levels.
- Local election officials in some jurisdictions may lack the staff, technology, and other resources to by themselves quickly deploy or repurpose new voting technology in time for the constitutionally scheduled general election, and many will request (or would welcome) outside (state or federal) assistance.

We focus here on identifying challenges for conducting broadly accessible, secure, robust elections under these conditions, as well as outlining possible approaches and technologies that could be deployed to assist local election officials.

BACKGROUND: ELECTIONS IN THE US

A consequence of our federalist system is that US elections are in practice highly decentralized, with each state responsible for setting its own standards and procedures for registering voters, casting ballots, and counting votes. The federal government has set only broad

[1] Professor and McDevitt Chair of Computer Science and Law, Georgetown University, 600 New Jersey Ave NW, Washington, DC 20001. *mab497@georgetown.edu.*

standards for such issues as accessibility, but has historically been largely uninvolved in day-to-day election operations. In most states, the majority of election management functions are delegated to local county and town governments, which are responsible for registering voters, procuring voting equipment, creating ballots, setting up and managing local polling places, counting votes, and reporting the results of each contest. Consequently, thousands of individual local election offices shoulder the burden of managing and securing the voting process for most of the American electorate. There are over 5000 local jurisdictions in the US with responsibility for conducting elections.

Elections in the US are among the most operationally and logistically complex in the world. Many jurisdictions have large numbers of geographically dispersed voters, and most elections involve multiple ballot contests and referenda. It is not uncommon for ballots to consist of 50 or 100 contests, and for many different ballot forms to be used for different voters within a county (e.g., for local representatives such as city council seats). Baseline election security must account for sophisticated adversaries, ballot secrecy, fair access to the polls, and accurate reporting of results, making secure election management one of the most formidable – and potentially fragile – information technology problems in government. This is true even under normal, undisrupted conditions.

An excellent overview of US elections (focused on security and integrity issues) is the recent NASEM consensus report "Securing the Vote".[2] It is especially useful as a baseline for understanding the many competing equities and tradeoffs at play here even under non-emergency conditions.

Computers and software play central roles in almost every aspect of our election process: managing voter registration records, defining ballots, provisioning voting machines, tallying and reporting results, and controlling electronic voting machines used at polling places.[3] The integrity and security of our elections are thus inexorably tied to the integrity and security of the computers and software that we rely on for these many functions, and to the ancillary processes and infrastructure that protect them.

The passage of the federal Help America Vote Act (HAVA) in 2002 accelerated the computerization of voting systems, particularly with respect to the ways in which voters cast their ballots at local polling stations. HAVA provided funds for states to replace precinct voting equipment with "accessible" technology. HAVA funding was a single sum that has, for the most part, been exhausted.

A. Voting Systems and Election System Infrastructure

A typical[4] county election office today depends on computerized systems and software

[2] https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy

[3] A typical election administration office is much like any modern enterprise, with local computer networks tying together desktop computers, printers, servers, and Internet access. This increasing connectivity served as a critical avenue in 2016 for what US intelligence agencies have identified as attacks by Russian military intelligence..

[4] The precise nature of the systems used and how they interact with one another will vary somewhat depending on the vendors from which the systems were purchased and the practices of the local jurisdiction.

for virtually every aspect of registering voters and conducting elections. Generally, an election office workflow will include at least the following pre- and post- election functions:

Voter registration – The ongoing maintenance of an authoritative database of registered voters in the jurisdiction, including the precinct-by-precinct “poll books” of voters (which might be on paper or in electronic form) that are used to check in voters at precinct polling stations.

Ballot definition – The pre-election process of creating data files that list the various contests, candidates, and rules (e.g., number of permitted choices per race) that will appear on the ballot. The ballot definition is used to print paper ballots, to define what is displayed on touchscreen voting terminals, and to control the vote tallying and reporting software. Local races (such as school boards) may sometimes require that different ballot definitions be created for different precincts within a county in any given election.

Voting machine provisioning – The pre-election process of configuring the individual precinct voting machines for an election. This typically includes resetting internal memory and loading the appropriate ballot definition for each precinct. Depending on the model of voting machine, provisioning typically involves using a computer to write removable memory cards that are installed in each machine.

Absentee and early voting ballot processing – The process of reading and tabulating ballots received by mail and from early voting polling places. Mail votes are typically processed in bulk by high-volume optical scan ballot reading equipment.

Tallying and reporting – The post-election process of tabulating the results for each race received from each precinct and reporting the overall election outcomes. This process typically involves using a computer to read memory card media retrieved from precinct voting machines.

Each of the above “back end” functions employs specialized election management software. Depending on the size and practices of the county, the same computers may be used for more than one function (e.g., the ballot definition computer might also serve as the tallying and reporting computer). These computers are typically off-the-shelf desktop machines running a standard operating system (such as Microsoft Windows), often equipped with electronic mail and web browser software along with the specialized voting software. Election office computers are typically connected to one another via a wired or wireless local area network, which may have a direct or indirect connection (sometimes via a firewall) to the Internet.

In some jurisdictions, some of these election management functions (most often those concerned with voter registration databases and ballot definition), may be outsourced by a county or state to an election services contractor. These contractors provide jurisdictions with specialized assistance with such tasks as creating ballots in the correct format, managing voter registration databases, creating precinct poll books, and maintaining voting machines. The degree to which jurisdictions rely on outside contractors varies widely across the nation. **It is not always the case, therefore, that all the expertise, technology, or resources required to conduct an election or implement emergency changes to election procedures will be available entirely “in house” with county government staff.**

It is often useful to divide the election technology and workflow landscape into two conceptual parts: *Voting Systems,* the technologies and processes on which votes are cast and recorded, and *Election Management Systems*, the "backend" functions that support voting but that do not themselves directly record or tabulate votes.

Backend election management systems comprise a major (and particularly exposed, often with a direct or indirect Internet connection) part of the election attack surface. While attacks against or failures of these systems may not be able to alter votes per se, there is a significant risk that a failure or compromise could result in of denial of service or disruption. For example, compromise of a voter registration database can prevent voters from voting or could cast doubt on the legitimacy of results. Voting systems, on the other hand, are even more critical, since an attack against or failure of them can affect election outcomes, in some cases with no way to recover the true result.

The integrity of the vote today thus increasingly depends on the integrity of multiple complex software systems and processes – including not just software running on voting machines but also on county election office networks – over which elections are conducted. Even under ideal circumstances, security weakness in any component of any of these systems can serve as a "weak link" that can allow a malicious actor to disrupt election operations, alter tally results, or disenfranchise voters. **Any hastily adopted last minute changes or additions to these systems add further potential to introduce subtle weaknesses or, equally importantly, create the perception that the integrity of the vote has been compromised**.

It is important to emphasize here that there is no "standard" software platform or configuration for election management. While there are a few commonly used software packages provided by voting system vendors, there is wide variation in the precise configuration and workflow across the over 5000 local election offices (generally counties and townships) in the nation. This represents a particular challenge to national disaster planning for elections, since there is no single "plug and play" system that can be guaranteed to interoperate with existing voter registration databases, ballot definitions, tallying, or reporting systems used in any given place.

The particular voting system technologies used vary from state to state, and sometimes from local jurisdiction to local jurisdiction within a state. Voting is conducted with one or more of the following methods:

- In-person voting on election day at local neighborhood precincts.
- In-person early voting prior to election day, often at a smaller number of "voting centers",
- Absentee or "vote-at-home" voting, typically via a paper ballot that is mailed to the voter and then returned by mail or dropped off at a collection center.

All US jurisdictions provide for absentee voting by mail for voters who will be out of town or who cannot travel to their designated polling place because of disability. Other jurisdictions permit any voter to request an mail-in ballot, but still provide for in-person voting.

A few jurisdictions (e.g., Oregon) rely primarily or exclusively on postal voting for the entire electorate.

It is worth noting that vote-by-mail represents a compromise between equities that are each regarded as fundamental to the US franchise. For example, it helps ensure the right to vote for those would be unable to otherwise, on the one hand, but it can degrade the right to a secret ballot, on the other. Because the ballot is simply delivered to the voter's home, there is no guarantee that the voter will be afforded privacy when completing and returning it. A spouse, child, parent, employer, or other party could, in principle, coerce a mail-in voter into voting a certain way, provide incentives to vote for a particular candidate, or purloin and complete the ballot without the voter's knowledge. These risks are generally regarded as a regrettable but acceptable tradeoff at small scale, but can become potentially problematic if vote-by-mail is suddenly widely deployed. Some jurisdictions currently rely heavily on vote-by-mail, and have made an explicit policy choice about these tradeoffs. Other jurisdictions have made other choices.

A productively useful, conservative approach for emergency voting is to focus on developing tools and processes to support an expansion of *existing* absentee voting capabilities, in a way that can be flexibly and rapidly deployed in the event that in-person voting is deemed infeasible or unsafe in jurisdictions that traditionally rely on it (and possibly with postal delivery services partly degraded). It is critical that any technology or processes developed be able to be integrated into existing voting workflow with minimal disruption or change, maximum transparency, and that the system be secure, robust, and accessible to as much of the electorate as possible. Public confidence in the integrity of the system is critical.

.

B. Absentee Voting Workflow and Logistics

Absentee voting by mail is conceptually simple, but entails a number of logistical challenges. It should be understood as a complex protocol, with security and robustness implications at many of its steps.

In jurisdictions that provide in-person precinct voting, voters requiring (or preferring) to vote by mail must generally explicitly request an absentee ballot before some deadline, which may be several weeks prior to the election, but in any case must allow sufficient time for processing, mailing, and return of the completed ballot before election day. The request must be authenticated by the county clerk or other official as coming from a currently registered voter in the jurisdiction. In some places, as part of this process the voter must certify that they have a lawfully valid reason for requesting an absentee ballot. In some places, this request can be made online; others required a signed paper form. Once authenticated, the ballot form package corresponding to the voter's registered address is mailed to either the registered address or an out-of-town address. The voter must also be removed from the pollbook used to check in voters at the precinct polling place, to prevent absentees from voting twice.

In jurisdictions that use exclusively vote-by mail, ballot packages are typically mailed to every voters' address of record unless a voter has asked that theirs be mailed elsewhere. Whether requests for a ballot to be sent to an alternative address can accommodated after the original ballot has been mailed depends on the particular jurisdiction, but generally will require the sending of a provisional ballot that will only be counted if the original ballot is found not to have been returned. Provisional ballots are also typically used when a voter complains that they did not receive the original ballot.

Ballots, or ballot instructions, as well as voter guides, often must be available in multiple languages, as well as large-print formats, to accommodate a diverse range of voters. Ballot design and layout is often tightly regulated, to ensure fairness to different candidates.

In many jurisdictions, completed ballots must be *received* by the election office by the time polls close on election day. It is effectively the *voter's* responsibility to mail the ballot in time to allow for it to travel through the postal system. (This can be particularly problematic for overseas voters.) In some jurisdictions, the voter must affix postage to mail the ballot; in others, a pre-paid return envelope is provided. In some jurisdictions, it is possible for a voter to confirm online that their returned ballot was received via a tracking number provided with the ballot.

Completed ballots are typically returned in two nested envelopes: an outer envelope, which contains a sealed inner envelope with the completed ballot. The outer envelope identifies the voter (possibly with a unique a serial number), and usually must be signed by the voter. Staff at the election office use the information on the outer envelope to authenticate the ballot and confirm that the signature matches a signature image for the voter on file. Once authenticated, the inner envelope is separated from the outer envelope and passed on for tabulation, now devoid of any information that identifies the voter.

Received ballot envelops might also be rejected by the election office, most commonly due to a missing signature or a signature mismatch. A signature mismatch does not, however, reliably indicate fraud. It is common for individuals' signatures to change over time, and ballot envelopes are not always conducive to consistent handwriting. Different jurisdictions (and different staff members) may apply inconsistently rigorous standards of comparison to ballot envelop signatures.

When an otherwise valid ballot is rejected, the voter must learn of the rejection (either by notification by mail or by checking online) and then must initiate a "curing" process to affirm that the ballot is truly theirs. The curing process varies from jurisdiction to jurisdiction according to local law. Commonly, the voter must complete an affidavit confirming that the ballot was theirs, possibly accompanied by documentation of identity. Sometimes this can be done by mail or online, but signature curing procedures vary across jurisdictions. A similar (though often more cumbersome) process also exists for authenticating provisional ballots before they are tallied.

Ballots that have been accepted for processing are generally tabulated using special high speed ballot scanners. Most ballot scanners employ "mark sense" optical scan technology that detects marks on the ballot based on the ballot definition configuration. Note that "spoiled" ballots (those in which a voter overvoted or undervoted in a race) cannot be corrected at this point, since by the time a ballot has been scanned and the error detected, it has already been decoupled from the identity of the voter. Absentee ballots often have a somewhat higher rate of spoilage than in-person voting for this reason.

Most (though not all) ballot scanning systems incorporate rudimentary security features to detect counterfeit ballot forms (such as those that might be produced by a consumer printer or photocopier). Ballots are typically pre-printed with a combination of infrared absorbing and infrared reflecting inks that must appear in specific places for the ballot to scan correctly. These systems require that ballots be produced by special printers with the capability to print the security features, and preclude the use of "print at home" or "print on demand" ballots on ordinary paper stock.

Observe that the integrity of elections based on mail-in-voting depends on both the integrity of software systems (particularly in ballot scanners) as well as rigorous physical controls to prevent unauthorized tampering with, destroying, or inserting, ballots. Because the software in ballot scanners cannot be adequately assured, post-election audits are now recommended to assure that the election outcome has been tallied correctly. The most common procedure for this is called a "Risk Limiting Audit", where a sample of ballots are selected and interpreted by hand, using a statistically rigorous process.[5] The effect of risk-limiting audits is not to eliminate software vulnerabilities, but to ensure that the integrity of the election outcome does not depend on the herculean task of securing every software component in the system. This important property is called *strong software independence*.[6] Software independence is regarded as an essential requirement for trustworthy elections.

A few companies have proposed app-based "solutions" for remote voting. The most prominent of these is Voatz, which has a blockchain-based system. App based (and internet-based) return of ballots is specifically warned against in the NASEM report, and exploitable flaws have recently been found in the Voatz system. West Virginia, an early user of Voatz, recently canceled its planned use of the system for shut-in voters.

RECOMMENDATIONS FOR MOVING FORWARD

Deploying any kind of emergency "vote-at-home" voting scheme across the nation on short notice will be extremely challenging. Even if a scheme were designed, reviewed, built and productized *today*, and the decision to employ it made immediately, the integration task across the more than 5000 voting jurisdictions in the US by itself would require aggressive action and significant support in order to have an impact on voting in the November 2020 general election. It is therefore imperative that any such system be designed conservatively, to introduce as little new technology as possible, and to integrate as seamlessly as possible with the highly varied existing election management infrastructure in place. In other words, any emergency system (and any centralized support) must follow, rather than lead, local practices.

[5] A good introduction to the theory and practice of risk limiting audits in elections can be found at https://www.stat.berkeley.edu/~stark/Preprints/RLAwhitepaper12.pdf .

[6] See Ron Rivest. "On the notion of 'software independence' in voting systems". *Phil. Trans Royal Society A*. Volume 366 Issue 1881. October 28, 2008. http://rsta.royalsocietypublishing.org/content/366/1881/3759 .

The most promising approach (likely the only viable approach given the legal, technical, and logistical constraints) is to develop agile systems to support scaling up the existing mail-in absentee ballot protocols already in use in every jurisdiction. Such a scheme would rely on physical delivery of ballots by the USPS or some other delivery service.

Even jurisdictions that currently support universal-vote-by-mail may face challenges, including, but not limited to:

- Possibly degraded postal delivery service, with increased delays, lost mail, etc.
- An increase in the number of address changes, due to voters in hospitals, quarantined outside their homes, or otherwise indisposed at some location other than home on election day.
- An increase in the number of provisional ballots, requiring increased manual processing.
- Diminished staff resources for handling voter inquiries, registering voters, processing received ballots, curing signature mismatches, and processing provisional ballots.

Jurisdictions that do not currently support universal-vote-by-mail (which comprise most of the US) may face the above challenges plus others, including:

- Printing of additional ballots on short notice, possibly too late to obtain ballots from printers who can incorporate the security features required by their bulk scanners.
- Scaling up bulk processing of centrally counted marked ballots.
- Increased pressure on centralized ballot storage and chain-of-custody controls.
- Getting accurate and timely information to voters about changes to voting procedures ahead of the election.

Provisional ballot processing in particular is notoriously difficult to scale. An emergency is likely to both increase the number of provisional ballots as well as put additional stress on the human and other resources required to process them.

USPS is likely to be an essential partner here, and it is important to involve them early rather than late. In particular, local post offices could be asked to prioritize mailed ballot handling (especially in the face of degraded service), assist with face-to-face interactions with voters, and manage scaled up ballot chain of custody processes.

End-to-End Verifiable Voting (e2e voting) techniques might be useful, but are in practice quite complex and not well understood by voters or election officials. The NASEM report (cited above) has useful perspective on the potential roles and limitations of e2e, mobile voting, and the Internet, and repays close attention.

Perhaps the most significant potential technological bottleneck, and an area that is likely to profit from rapid development and deployment, is ballot printing and scanning. COTS printers for on-demand and bulk ballot printing could be fielded in the absence of timely commercial ballot printing capability. This would need to be accompanied by compatible bulk scanning hardware and software, preferably based on COTS hardware. It would be important to identify printing and scanning hardware quickly, to ensure that it could be procured and available for fielding in sufficient quantities ahead of the general election.

Ballot definition and design is a non-trivial task in practice, even if it sounds conceptually simple. Local jurisdictions will require time and training to create usable ballots on any new system. They must also train staff and communicate with voters about precisely how they will vote. This means systems need to be in their hands by August or September at the latest.

For any emergency system to have a chance at success, it must be designed in partnership with experts in the varied idiosyncrasies of election law across the country. It is likely that no single system is compatible with the requirements of election law in all 50 states plus territories. Flexibility and agility are central requirements here.

The accessibility requirements of HAVA are neither trivial nor optional. Even with a widespread expansion of mail voting, jurisdictions will still likely need to provide for in-person voting in some form for some voters (including those with certain disabilities, language issues, or without stable mail delivery).

Some jurisdictions will resist or mistrust offers of federal help, for political or cultural reasons.

Given the experiences of 2016, disruption and denial of service from foreign and domestic actors must figure prominently in the threat model.

Transparency is critical. Any new system will be relentlessly scrutinized and attacked, especially by supporters of whoever loses the election. High assurance hardware and software may play a role, but is not a substitute for software independence. (Compatibility with Risk Limiting Audits is essential). The legitimacy of the election depends not just on the actual security properties of the system, but on public perception of those properties.