CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE NOTE

July 28, 2020; 1530 EDT.

MAIL-IN VOTING IN 2020 INFRASTRUCTURE RISK ASSESSMENT

Each method of voting carries risks that election officials must manage. This risk assessment is designed to assess the risks to the mail-in-voting election systems, processes, and infrastructure to inform states, localities, and industry. [i] This risk assessment only examines the specific risks to the election infrastructure and operations that are associated with mail-in voting.

For the November 2020 election, the COVID-19 pandemic will likely impact voters' voting patterns. Many states and jurisdictions have modified their processes and infrastructure to address the change in the environment to include considerations of how to utilize mail-in voting.

KEY FINDINGS

All forms of voting – in this case mail-in voting – bring a variety of cyber and infrastructure risks. Risks to mail-in voting can be managed through various policies, procedures, and controls.

The outbound and inbound processing of mail-in ballots introduces additional infrastructure and technology, which increases the potential scalability of cyber attacks. Implementation of mail-in voting infrastructure and processes within a compressed timeline may also introduce new risk. To address this risk, election officials should focus on cyber risk management activities, including access controls and authentication best practices when implementing expanded mail-in voting.

Integrity attacks on voter registration data and systems represent a comparatively higher risk in a mail-in voting environment when compared to an in-person voting environment. This is because the voter is not present at the time of casting the ballot and cannot help to answer questions regarding their eligibility or identity verification.

Operational risk management responsibility differs with mail-in voting and in-person voting processes. For mail-in voting, some of the risk under the control of election officials during in-person voting shifts to outside entities, such as ballot printers, mail processing facilities, and the United States Postal Service (USPS).

Physical access at election offices and warehouses represents a risk in a mail-in voting environment. Completed ballots are returned to the election office and must be securely stored for days or weeks before processing through voter authentication and tabulation processes. Managing risks to these processes requires implementing secure procedures for storage, access controls, and chain of custody, such as ballot accounting.

Inbound mail-in ballot processes and tabulation take longer than in-person processing, causing tabulation of results to occur more slowly and resulting in more ballots to tabulate following election night. Media, candidates, and voters should expect less comprehensive results on election night, which creates additional risk of electoral uncertainty and confidence in results.

Disinformation risk to mail-in voting infrastructure and processes is similar to that of in-person voting while utilizing different content. Threat actors may leverage limited understanding regarding mail-in voting processes to mislead and confuse the public.

[i] This risk assessment serves as a companion to CISA's *Election Infrastructure Cyber Risk Assessment* and the *Risk Management for Electronic Ballot Delivery, Marking, and Return* that CISA jointly released in May 2020 with the Election Assistance Commission, the National Institute of Standards and Technology, and the Federal Bureau of Investigation.

SCOPE NOTE: The Cybersecurity and Infrastructure Security Agency (CISA) prepared this risk assessment to support CISA efforts to help U.S., state, and local governments identify and mitigate vulnerabilities to mail-in voting infrastructure, and support physical security, cybersecurity, and operational resilience within the mail-in voting process. This product provides base-level analysis election officials can use to prioritize and tailor risk management efforts to address specific vulnerabilities in high consequence mail-in voting processes and infrastructure, and to promote resilience within supporting election systems. This document is not an endorsement of any election management practice. Prioritizing mitigating risk to the mail-in voting infrastructure and processes could yield the greatest marginal benefit in improving states' risk profiles.

RISK AND COMPENSATING CONTROLS OVERVIEW

TABLE 1—RISK AND COMPENSATING CONTROLS WITHIN MAIL-IN VOTING INFRASTRUCTURE AND PROCESSES

RISK	COMPENSATING CONTROLS
All forms of voting – in this case mail-in voting – bring a variety of cyber and infrastructure risks. Risks to mail-in voting can be managed through various policies, procedures, and controls.	When implemented properly, mail-in voting has a series of layered safeguards to defend the process from manipulation. Similar to in-person voting a voter must be registered to vote before receiving a ballot. The voter is validated (i.e., signature, ID, witness, notary, etc.) before a ballot package is accepted. A ballot is then separated from the ballot package for voter privacy. The envelopes are kept, designating that the voter has voted (in case they try to double vote) and the ballot is counted.
Implementation of mail-in voting infrastructure and processes within a compressed timeline may also introduce new risk.	Election officials are natural risk managers. They must assess the risks of introducing new infrastructure with the operational risks associated with doing so in a compressed timeline before making a determination. Planning, preparation, training, and redundancy (i.e., paper backups) will build resiliency.
Operational risk management responsibility differs with mail-in voting and in-person voting processes. For mail-in voting, some of the risk under the control of election officials during in-person voting shifts to outside entities, such as ballot printers, mail processing facilities, and the USPS.	Vendor Safeguards: Election officials are requiring their private sector partners to implement physical and cyber safeguards to manage risk. The private sector partners are implementing technical and procedural best practices and are integrated in the information sharing and analysis center to identify threats and manage risks to the election infrastructure. USPS Election Mail Program Safeguards: USPS has a dedicated election mail program to aid in envelope design to, in coordination with the state, safeguard the chain of custody for ballots in transit. The election mail program includes an intelligent mail barcoding (IMB) system enabling ballot tracking.
Integrity attacks on voter registration data and systems represent a comparatively higher risk in a mail-in voting environment when compared to an in-person voting environment. This is because the voter is not present at the time of casting the ballot and cannot help to answer questions regarding their eligibility or identity verification.	Many jurisdictions have a cure process where they contact a voter if a signature or ID is missing, does not match, or if there are other reasons for rejecting the ballot package. If a voter does not receive a ballot because the information is incorrect (i.e. incorrect name, address, etc.) the voter has the opportunity to go to a voting location and vote a provisional ballot.
The outbound processing of mail-in ballots introduces additional infrastructure and technology, providing new potential opportunities for cyber attacks.	To address this risk, election officials should focus on cyber risk management activities, including proper configuration, access controls, and authentication best practices when implementing mail-in voting.

RISK	COMPENSATING CONTROLS
The inbound processing of mail-in ballots introduces additional infrastructure and technology, providing new potential opportunities for cyber attacks.	Cyber security best practices must be implemented to manage the risk to election technology and infrastructure. Increasing the amount of infrastructure and technology expands the vectors of attack for cyber actors and opportunity to affect the process at scale. However, the compensating controls are the same as other election technology and infrastructure. Election officials have been implementing mechanism to protect, detect, respond, and recover to build resiliency in the overall election process.
Electronic ballot return is high risk. Electronic ballot return, the digital delivery of a voted ballot back to the election authority, faces significant security risks to voted ballot integrity, voter privacy, and system availability.	There are no compensating controls to manage electronic ballot return risk using current technologies. While many risks associated with electronic ballot return have a physical analog with the risk associated with the mailing of ballots, the comparison can miss that electronic systems provide the opportunity to rapidly affect voting at scale. For assessment of the risks associated with the electronic delivery, marking, and return of ballots, refer to *Risk Management for Electronic Ballot Delivery, Marking, and Return (May 2020).*
Jurisdictions may need additional infrastructure or processes to tabulate mail-in ballots, such as central count machines or use precinct scanners to scan ballots which may require a significant amount of human capital, space, and administrative controls.	Cyber security best practices must be implemented to manage the risk of election technology and infrastructure. Increasing the amount expands the vectors of attack for cyber actors and opportunity to affect the process at scale. However, the compensating controls are the same as other election technology and infrastructure. Election officials have been implementing mechanisms to protect, detect, respond, and recover to build resiliency in the overall election process.
Inbound mail-in ballot processes and tabulation take longer than in-person processing, causing tabulation of results to occur more slowly and resulting in more ballots to tabulate following election night. Media, candidates, and voters should expect less comprehensive results on election night, which creates additional risk of electoral uncertainty and confidence in results.	Some jurisdictions have implemented election technology and infrastructure to speed up the process (i.e., mail sorting equipment, electronic signature verification systems, central count scanning systems, etc.). Some jurisdictions are legally afforded the opportunity to begin processing ballot application and ballots in advance of Election Day, similar to early voting. Election officials, media, candidates, and non-governmental organizations are working collaboratively to educate voters and set the expectations that the results on election night will be less comprehensive and it will take days, if not weeks, to determine the outcome of many races.
Disinformation risk to mail-in voting infrastructure and processes is similar to that of in-person voting while utilizing different content. Threat actors may leverage limited understanding regarding mail-in voting processes to mislead and confuse the public.	Election officials, media, candidates, and non-governmental organizations are working collaboratively to educate voters about the mail in voting process, including voter registration deadlines, mail in ballot application requirements, deadline for sending and/or receiving a ballot, voter verification process and requirements (i.e., signature, ID, witness, notarize, etc.), delayed tabulation and reporting expectations, etc. The National Association of Secretaries of State (NASS) launched #TrustedInfo2020—a new education effort to promote election officials as the trusted sources of election information. #TrustedInfo2020 aims to highlight state and local election officials as the credible, verified sources for election information.

MAIL-IN VOTING ELECTION INFRASTRUCTURE OVERVIEW

Election infrastructure includes a diverse set of systems, networks, and processes. Mail-in voting is a method of administering elections. When voting by mail, authorized voters receive a ballot in the mail, either automatically or after the application process. In most implementations, the voter marks the ballot, puts the ballot in an envelope, signs an affidavit, and returns the package via mail or by dropping off at a ballot drop box or other designated location.

Currently, five states (Colorado, Hawaii, Oregon, Utah, and Washington) automatically send every registered voter a ballot by mail. At least 21 other states have laws that allow at least some elections to be conducted by mail. In addition to the five states that send every voter a ballot, five states (Arizona, California, Montana, Nevada, and New Jersey) and the District of Columbia (D.C.) allow a voter to apply to receive a mail-in ballot permanently, so that voters do not have to apply each election.[1] Currently, 34 states and D.C. allow any registered voter to request a mail-in ballot. There are 16 states that require voters to have an excuse such as temporary absence from the voting district, illness, or disability or require voters to be of a certain age (typically 65+) to be eligible to receive a ballot by mail. Some states are recognizing COVID-19 as a valid excuse.

Although they perform similar functions, mail-in voting processes and infrastructure vary from state to state and often differ even between counties, parishes, towns, or cities within a state or territory. While each state manages and conducts mail-in elections differently based on state and local legal requirements, common risks and mitigations exist across states and implementations.

Figure 1 provides a functional overview of the process for mail-in voting. Each of the following sections of this assessment describe detailed risks per mail-in voting infrastructure system or process step, followed by the related key finding and compensating controls. Detailed information about compensating controls for specific sub-steps of the process is included in Table 2.

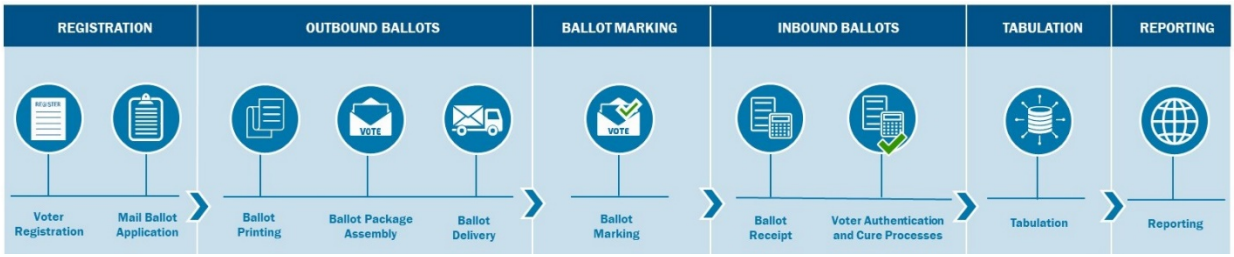

FIGURE 1—MAIL-IN VOTING PROCESS

MAIL-IN VOTING ELECTION INFRASTRUCTURE AND PROCESS RISK

All forms of voting – in this case mail-in voting – bring a variety of cyber and infrastructure risks. Risks to mail-in voting can be managed through various policies, procedures, and controls. The outbound and inbound processing of mail-in ballots introduces additional infrastructure and technology, introducing new or additional potential vectors for cyber attacks and increasing the opportunity for cyber actors to impact the infrastructure at scale. Implementation of mail-in voting infrastructure and processes within a compressed timeline may also introduce new risk. To address this risk, election officials should focus on cyber risk management activities, including effective access controls and authentication best practices.

While compromises to ballots present a high consequence target for threat actors, the low likelihood and scale of attacks on ballots while in-transit[ii] means there is lower risk than attacks during other stages, such as outbound (e.g., ballot package assembly) and inbound (e.g., ballot receipt) processes.

[ii] In-Transit is generally considered the time after a ballot has left the jurisdiction, but before the voter receives ballot, or after the voter has returned the ballot, but before the jurisdiction has received it.

Each of the following sections describe our findings organized by mail-in voting infrastructure system or process step, followed by the related key finding and compensating controls.

RISK	COMPENSATING CONTROLS
All forms of voting – in this case mail-in voting – bring a variety of cyber and infrastructure risks. Risks to mail-in voting can be managed through various policies, procedures, and controls.	When implemented properly, mail-in voting has a series of layered safeguards to defend the process from manipulation. Similar to in-person voting a voter must be registered to vote before receiving a ballot. The voter is validated (i.e., signature, ID, witness, notary, etc.) before a ballot package is accepted. A ballot is then separated from the ballot package for voter privacy. The envelopes are kept to designate that the voter has voted (in case they try to double vote) and the ballot is counted.
Implementation of mail-in voting infrastructure and processes within a compressed timeline may also introduce new risk.	Election officials are natural risk managers. They must assess the risks of introducing new infrastructure with the operational risks associated with doing so in a compressed timeline before making a determination. Planning, preparation, training, and redundancy (i.e., paper backups) will build resiliency.
Operational risk management responsibility differs with mail-in voting and in-person voting processes. For mail-in voting, some of the risk under the control of election officials during in-person voting shifts to outside entities, such as ballot printers, mail processing facilities, and the United States Postal Service (USPS).	Vendor Safeguards: Election officials are requiring their private sector partners to implement physical and cyber safeguards to manage risk. The private sector partners are implementing technical and procedural best practices and are integrated in the information sharing and analysis center to identify threats and manage risks to the election infrastructure. USPS Election Mail Program Safeguards: USPS has a dedicated election mail program to aid in envelope design to, in coordination with the state safeguard the chain of custody for ballots in transit. The election mail program includes an intelligent mail barcoding (IMB) system enabling ballot tracking.

Voter registration and mail ballot application processing collects data used to determine voter eligibility, the type of ballot a voter receives, the location or address for mailing the ballot to the voter, and whether election officials can accept the ballot. Either an integrity attack or an availability attack on a voter registration system could result in a voter not being able to cast a ballot or a voter's ballot not being counted. Integrity attacks on voter registration data and systems represents a comparatively higher risk in a mail-in voting environment than an in-person voting environment. This is because the voter is not present at the time of casting the ballot and cannot help to resolve questions regarding eligibility or verification. Mail-in voters whose registration records are altered or deleted in an integrity attack do not have the opportunity to be issued a provisional ballot, which are available to in-person voters.

- An integrity attack that removed a voter from the voter registration, permanent mail, or absentee ballot request list could result in the voter not receiving a ballot, unless the voter proactively followed up to re-register, re-apply, or if the election official received the ballot as undeliverable and contacted the voter. The impact is that a voter may not receive a ballot or receipt of a ballot may be delayed, resulting in a jurisdiction potentially not accepting a voted ballot. The voter would still possess the ability to vote in person provisionally.
- An integrity attack on a voter's name could result in the voter receiving a ballot package that is not addressed to the proper individual. If there was an integrity attack on a voter's identifying information (i.e., date of birth [DOB], driver's license number [DL], last four digits of Social Security number [SSN], etc.), the voter's proof of ID, where required, would not match the voter's record. The voter would either need to inform the election official and update his or her voter record (assuming that the voter registration deadline has not passed), or risk having their voted ballot rejected upon receipt.
- An integrity attack on a voter's ballot mailing address may result in the voter not receiving a ballot, unless the voter proactively updated his or her registration with the correct address, or the election official received the ballot as undeliverable and contacted the voter. This assumes that the voter registration or ballot application deadline has not passed, allowing the voter to update his or her information. The impact is that a voter may not receive a ballot, or receipt of a ballot is delayed.
- An integrity attack on a voter's signature on file could result in the voter having the ballot package rejected and their ballot uncounted. If the state is one of the 19 that requires a voter to receive

notification when there is a discrepancy with their signature or the signature on the return ballot envelope is missing (a.k.a. "cure process"), the voter may have an opportunity to correct the situation by being notified that the ballot was rejected and taking action to resolve the issue.[2] This can be done by an election official notifying the voter or a voter checking a ballot tracking system, if available.

- An availability attack on the voter registration database or specific information, such as a list of mail voters, voter names, or addresses could result in the delay of voters receiving their ballots, and further impact voters' ability to return ballots on time to ensure they are counted. In most states, a ballot may be returned in person, in which case the impact of an availability attack may only affect the outbound process providing a measure of resilience.

RISK	COMPENSATING CONTROLS
Integrity attacks on voter registration data and systems represent a comparatively higher risk in a mail-in voting environment when compared to an in-person voting environment. This is because the voter is not present at the time of casting the ballot and cannot help to answer questions regarding their eligibility or identity verification.	Many jurisdictions have a cure process where they contact a voter if a signature or ID is missing, does not match, or if there are other reasons for rejecting the ballot package. If a voter does not receive a ballot because the information is incorrect (i.e. incorrect name, address, etc.) the voter has the opportunity to go to a voting location and vote a provisional ballot.

Outbound ballot processing in a mail-in voting environment consists of printing ballots, assembling ballot packages, and mailing ballots to a voter. Generally, this process is outsourced to external entities, which shifts the risk under the control of election officials during in-person voting to outside entities, such as ballot printers, mail processing facilities, and USPS. Physical security for the outbound ballot process is crucial. In-house processing of outbound ballots is a manual and labor-intensive process in which personnel fold, stuff, seal, label, and ship ballots.

- **Ballot Printing:** Almost all election jurisdictions use a ballot printer to print their ballots. Election officials send ballot printers electronic copies of ballot files for printing. Without properly implemented security controls, the transmission of ballot files can be at risk to a person-in-the-middle (PITM) attack. A PITM attack may result in ballot files being altered before being printed, assembled, and shipped.
    - Ballot printers and mailing houses store ballot and voter data, such as names and addresses of voters, ballot styles, and in some cases voter history data. An integrity or availability attack to the third-party infrastructure could have the same impact as an integrity or availability attack, respectively, on voter registration databases.
- **Ballot Package Assembly:** The ballot package assembly process matches a voter to a ballot. Whether automated or manual, the risk to the process of assembling ballot packages lies in associating the voter with an incorrect ballot style and ballot mailing address, resulting in a voter receiving the wrong ballot.
- **Ballot Delivery:** Ballots will be delivered as official election mail if jurisdictions coordinate with USPS to ensure their ballot packages are compliant with election mail standards. Additionally, an integrity or availability attack to divert or slow delivery of mail ballots could impact voters' ability to return ballots on time to ensure they are counted.

RISK	COMPENSATING CONTROLS
The outbound processing of mail-in ballots introduces additional infrastructure and technology, providing new potential opportunities for cyber attacks.	To address this risk, election officials should focus on cyber risk management activities, including proper configuration, access controls, and authentication best practices when implementing mail-in voting.

Inbound ballot processing is comprised of receiving a voted ballot from a voter, as well as authenticating a voter to determine if their ballot will be accepted for tabulation. Ballots may be received weeks before Election Day until days after Election Day, depending on state law. Election jurisdictions must have enough secure

physical space to store received ballots until they are processed. State law dictates when election officials can begin processing ballots, allowing election officials to authenticate voters, accept or reject ballot packages, and separate ballots from the envelope for scanning. Chain of custody processes are crucial to tracking the amount and storage location of received ballots.

- In a mail-in voting model, election offices and storage facilities are used to store returned ballots and mail processing equipment, and to conduct inbound and outbound ballot processing. Election offices are locations where election officials conduct official business, including shared workspaces such as public libraries, municipal buildings, and other public areas. Election offices and warehouses represent a physical security risk in a mail-in voting environment. Chain of custody and physical security can play a critical role in managing risks to election facilities. Completed ballots are returned to the election office and must be securely stored for days or weeks before processing through voter authentication and tabulation processes. Managing risks to these processes requires implementing secure procedures for storage, access controls, and chain of custody, such as ballot accounting.
- For jurisdictions that leverage automated processes, additional infrastructure required for automation brings cyber risk. This additional infrastructure, such as mail ballot sorters, can be networked to the voter registration database in some implementations, or are networked to the internet to allow vendors to troubleshoot issues remotely. This additional networking introduces cyber risk into election processes and systems and should be properly managed.
- For jurisdictions that do not have the mail opening, sorting, and extracting machines or the technologies to authenticate the voter (e.g., signature verification systems), the inbound process is a manual and labor-intensive process requiring different allocation of personnel for ballot processing.
- Unlike in-person voting where there are processes to resolve an issue in real time through resiliency measures (such as provisional ballots or, where available, same day registration), mail-in voting does not offer similar processes for resiliency. The authentication mechanism for mail-in voting is generally the matching of a signature on the envelope to a voter's signature in the database. Some jurisdictions check the voter's name, DOB, DL, or SSN in addition to or in lieu of a signature. If the information does not match, the ballot may not be counted. A few jurisdictions have a cure process that allows a voter to correct the issue and ensure their ballot is counted (e.g., signing an unsigned envelope, providing proof of address, or attesting a signature is the voter's signature). State laws or rules determine when that cure process can occur. Some must be cured by Election Day while others allow periods of time, such as 3, 5, 8, or even 14 days after Election Day.

RISK	COMPENSATING CONTROLS
The inbound processing of mail-in ballots introduces additional infrastructure and technology, providing new potential opportunities for cyber attacks.	Cyber security best practices must be implemented to manage the risk to election technology and infrastructure. Increasing the amount of infrastructure and technology expands the vectors of attack for cyber actors and opportunity to affect the process at scale. However, the compensating controls are the same as other election technology and infrastructure. Election officials have been implementing mechanisms to protect, detect, respond, and recover to build resiliency in the overall election process.

Electronic ballot delivery, marking, and return systems cross portions of the outbound and inbound process. They are used for certain groups of voters, particularly military and overseas voters, that face challenges voting both in-person or through the mail. All jurisdictions are required to offer electronic ballot delivery for military and overseas voters, per federal law. Thirty-one states[iii] and D.C. allow voters covered by the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) (or a subset of those voters) to use electronic ballot return, such as internet portal, email, or fax.[3,4,5] Of those, nineteen states[iv] and D.C. allow some voters to use electronic ballot return via email or fax, while seven[v] states only allow electronic ballot return via fax. Six states

[iii] The 31 states are: Alaska, Arizona, California, Colorado, Delaware, Florida, Hawaii, Idaho, Indiana, Iowa, Kansas, Louisiana, Maine, Massachusetts, Mississippi, Missouri, Montana, Nebraska, Nevada, New Jersey, New Mexico, North Carolina, North Dakota, Oklahoma, Oregon, Rhode Island, South Carolina, Texas, Utah, Washington, and West Virginia.
[iv] The 19 states are: Delaware, Hawaii, Idaho, Indiana, Iowa, Kansas, Maine, Massachusetts, Mississippi, Montana, Nebraska, Nevada, New Jersey, New Mexico, North Carolina, Oregon, South Carolina, Utah, and Washington.
[v] The seven states are: Alaska, California, Florida, Louisiana, Oklahoma, Rhode Island and Texas.

(Arizona, Colorado, Delaware, Missouri, North Dakota, and West Virginia) allow UOCAVA voters to use electronic ballot return via a web-based portal or applications. Additionally, several jurisdictions across Utah, Colorado, Washington, New Jersey, and Oregon used these systems for non-federal elections and are determining their use moving forward.[6,7]

RISK	COMPENSATING CONTROLS
Electronic ballot return is high risk. Electronic ballot return, the digital delivery of a voted ballot back to the election authority, faces significant security risks to voted ballot integrity, voter privacy, and system availability.[8]	There are no compensating controls to manage electronic ballot return risk using current technologies. While many risks associated with electronic ballot return have a physical analog with the risk associated with the mailing of ballots, the comparison can miss that electronic systems provide the opportunity to rapidly affect voting at scale. For assessment of the risks associated with the electronic delivery, marking, and return of ballots, refer to *Risk Management for Electronic Ballot Delivery, Marking, and Return (May 2020).*

Centralized **vote tabulation and aggregation systems** are used to tally votes shared by sub-jurisdictions such as counties and precincts. These systems collect and process data to determine the result of an election contest. Tabulation encompasses both technology and processes used to count votes and aggregate results. Vote tabulation processes for mail-in voting include hand counting and optical scans of paper ballots. Mail-in voting tabulation typically occurs in a centralized location.

RISK	COMPENSATING CONTROLS
Jurisdictions may need additional infrastructure or processes to tabulate mail-in ballots, such as central count machines or use precinct scanners to scan ballots which may require a significant amount of human capital, space, and administrative controls.	Cyber security best practices must be implemented to manage the risk of election technology and infrastructure. Increasing the amount expands the vectors of attack for cyber actors and opportunity to affect the process at scale. However, the compensating controls are the same as other election technology and infrastructure. Election officials have been implementing mechanisms to protect, detect, respond, and recover to build resiliency in the overall election process.

Election night reporting for mail-in voting is significantly different. Inbound mail-in ballot processes and tabulation take longer than in-person processing, causing tabulation of results to occur more slowly and resulting in more ballots to tabulate following election night. Media, candidates, and voters should expect less comprehensive results on election night. In a mail-in voting environment, there may be a significant amount of unprocessed or uncounted mail ballots on election night which will make unofficial results less comprehensive than for in-person voting. Other than the tabulation process taking longer, the mail-in nature of the election should not impact the manner in which certified results are conveyed to the public.

RISK	COMPENSATING CONTROLS
Inbound mail-in ballot processes and tabulation take longer than in-person processing, causing tabulation of results to occur more slowly and resulting in more ballots to tabulate after election night. Media, candidates, and voters should expect less comprehensive results on election night, which creates additional risk of electoral uncertainty and confidence in results.	Some jurisdictions have implemented election technology and infrastructure to speed up the process (i.e., mail sorting equipment, electronic signature verification systems, central count scanning systems, etc.). Some jurisdictions are legally afforded the opportunity to begin processing ballot application and ballots in advance of Election Day, similar to early voting. Election officials, media, candidates, and non-governmental organizations are working collaboratively to educate voters and set the expectation that the results on election night will be less comprehensive and it will take days, if not weeks, to determine the outcome of many races.

Table 2 provides a high-level overview of the potential attack consequences within the mail-in voting process.

TABLE 2—CONSEQUENCES WITHIN THE MAIL-IN VOTING PROCESS

ELECTION PROCESS POTENTIAL ATTACKS	CONFIDENTIALITY CONSEQUENCE	INTEGRITY CONSEQUENCE	AVAILABILITY CONSEQUENCE
Voter Registration	Expose non-public voter registration information	Change voter record to deliver ballots to the incorrect location, provide voters incorrect ballots, delay delivery, or prevent or delay acceptance of voter ballot upon return	Prevent access to voter registration information needed to get the correct ballot to the voter on time, or to accept the ballot upon return
Ballot Application	Expose non-public voter personally identifiable information (PII) during the application process	Change voter information to delay or prevent the correct ballot from getting to the voter on time	Prevent access to ballot application information, preventing the correct ballot from getting to the voter on time
Ballot Printing	Expose voter PII during ballot printing	Change ballot information	Prevent access to ballot printing files or systems to delay printing
Ballot Package Assembly	Expose voter PII during ballot packaging	Change ballot package information to deliver to incorrect location, provide voter incorrect ballot, or delay delivery	Prevent timely assembly of ballot packages
Ballot Delivery	Expose non-public voter registration information during delivery	Change ballot address resulting in ballot being delivered to the incorrect voter or location	Prevent timely delivery of ballots to voters
Ballot Receipt	Expose voter ballot choices	Change voter ballot choices Prevent delivery of voted ballots to election officials	Prevent or delay delivery of voted ballots to election officials
Voter Authentication & Cure	Expose voter PII and signature	Change voter records so name or signature are incorrect to prevent or delay acceptance of ballots	Prevent or delay authentication of voters, delaying acceptance of ballots
Tabulation	Expose election results before release	Change tabulation of voter ballot choices	Prevent timely tabulation of ballots
Reporting	Expose election reporting results before release	Change unofficial reporting of election results	Prevent reporting of results

Table 3 provides specific compensating controls for the mail-in voting process.

TABLE 3—COMPENSATING CONTROLS WITHIN THE MAIL-IN VOTING PROCESS

	COMPENSATING CONTROL	DESCRIPTION	IN-PERSON EQUIVALENCY
PROCEDURAL CONTROLS	Ballot packages/ envelopes	Most states coordinate with USPS to designate the ballot packages/envelopes as "Official Election Mail" to authenticate it is from an election official.	None
PROCEDURAL CONTROLS	Signature attestation	In many states, ballot packages must be signed by the voter, attesting under penalty of perjury that the voter is the entity that filled out the ballot and who is "casting" (i.e., sending) the ballot to the election official.	A voter announces her or his name and address and signs a poll book attesting that they are said voter.
PROCEDURAL CONTROLS	Signature verification	In many states, the signature is verified manually or by using technology against a signature(s) that are on file. Note that in most states, this is not a single check and there is an escalation process before the ballot is rejected.	Voters sign the poll book. However, there is not a similar process for verifying the in-person signatures.
PROCEDURAL CONTROLS	Voter validation	In some states, a voter's identity must be validated before the ballot is extracted from the ballot package and allowed to proceed to the tabulation process (i.e., driver's license, ID card, voter registration card, etc.).	This process is the same for states with voter ID requirements.
PROCEDURAL CONTROLS	Voter authentication	In some states, a voter must be authenticated by having a witness sign the ballot envelope/package or by having it notarized.	There is no pre-authentication equivalency. Some states have the opposite where an in-person voter's identity can be challenged.
PROCEDURAL CONTROLS	Cure process	In some states, if the voter cannot be validated or authenticated, the voter is contacted to verify that the ballot package was submitted by her or him.	This would be similar to the provisional ballot process whereby an additional round of checks is conducted before the ballot is accepted or rejected.
PHYSICAL BALLOT CONTROLS	Ballot style codes	Most ballots have style codes (i.e. timing marks, code channels, QR codes, etc.) that are validated by the voting machines. Generally, these are in a proprietary format and can only be interpreted by a specific type of voting machine. If the codes are not recognized by the equipment, the ballot is rejected by the voting machine and manually reviewed by the election official.	N/A
PHYSICAL BALLOT CONTROLS	Ballot paper specifications	Most ballots must be printed on a specific type of paper. If the ballot is printed on paper that does not match the specifications (i.e. length, paper weight, opacity, etc.), the voting machine will reject the ballot.	N/A
PHYSICAL BALLOT CONTROLS	Ballot watermarks	Some voting systems and some states implement watermarks to be printed on the ballot that are specific to an election or designate it as being printed by an approved printing authority providing a visual cue that the ballot is authentic.	N/A

JOINT ELECTION INFRASTRUCTURE AND DISINFORMATION ATTACKS

Disinformation and mal-information risk to mail-in voting infrastructure and processes are similar to that of in-person voting while utilizing different content. Mail-in voting has already become an issue among partisan political voices, which makes it a target for threat actors to exploit in terms of pushing. These threat actors may mislead and confuse the public about the mechanics of mail-in voting, and leverage limited understanding regarding mail-in voting processes, in order to cause chaos and provoke distrust in the election administration and electoral results. For example, processing mail-in ballots can take a longer period of time when jurisdictions are not able to begin processing them until Election Day, or after the polls close. This will cause delays in getting results out to the public. Threat actors may exploit a delay in results to sow discord, manipulate public discourse, and discredit the electoral system, all to undermine the U.S. democratic system. To mitigate the risk of disinformation, voters should receive accurate information about mail-in voting to increase their understanding of the process along with reminders to rely on authoritative sources such as their state and local election officials when questions arise.

RISKS	COMPENSATING CONTROLS
Disinformation risk to mail-in voting infrastructure and processes is similar to that of in-person voting while utilizing different content. Threat actors may leverage limited understanding regarding mail-in voting processes to mislead and confuse the public.	Election officials, media, candidates, and non-governmental organizations are working collaboratively to educate voters about the mail in voting process, including voter registration deadlines, mail in ballot application requirements, deadline for sending and/or receiving a ballot, voter verification process and requirements (i.e., signature, ID, witness, notarize, etc.), delayed tabulation and reporting expectations, etc. The National Association of Secretaries of State (NASS) launched #TrustedInfo2020—a new education effort to promote election officials as the trusted sources of election information. #TrustedInfo2020 aims to highlight state and local election officials as the credible, verified sources for election information.

The Cybersecurity and Infrastructure Security Agency (CISA), National Risk Management Center (NRMC), is the planning, analysis, and collaboration center working in close coordination with the critical infrastructure community to Identify; Analyze; Prioritize; and Manage the most strategic risks to National Critical Functions. These are the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof. NRMC products are visible to authorized users at HSIN-CI and Intelink. For more information, contact Central@cisa.gov or visit https://www.cisa.gov/national-risk-management.

PDM 20063

[1] National Conference of State Legislatures, "States with Permanent Absentee Voting for All Voters, Voters with Permanent Disabilities and/or Senior Voters," April 27, 2020. https://www.ncsl.org/research/elections-and-campaigns/vopp-table-3-states-with-permanent-absentee-voting-for-all-voters-voters-with-permanent-disabilities-and-or-senior-voters.aspx. Accessed May 5, 2020.
[2] Cybersecurity and Infrastructure Security Agency Joint COVID Working Group, "Signature Verification and Cure Process," 2020, page 5. https://www.cisa.gov/sites/default/files/publications/signature-verification_cure_process_final_508.pdf. Accessed May 14, 2020.
[3] U.S. Election Assistance Commission, "Election Administration and Voting Survey: 2018 Comprehensive Report," 2018, page 15. https://www.eac.gov/sites/default/files/eac_assets/1/6/2018_EAVS_Report.pdf. Accessed May 14, 2020.
[4] National Conference of State Legislatures, "Electronic Transmission of Ballots," September 5, 2019. https://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx. Accessed April 27, 2020.
[5] Ibid.
[6] Associated Press, "2 Oregon counties offer vote-by-mobile to overseas voters," October 26, 2019. https://apnews.com/8ce0fbc400514f55839fa84fb364d7f4. Accessed May 14, 2020.
[7] Wall Street Journal, "Some States Dabble in Online Voting, Weighing Pandemic Against Cybersecurity Concerns," May 4, 2020. https://www.wsj.com/articles/some-states-dabble-in-online-voting-weighing-pandemic-against-cybersecurity-concerns-11588596299. Accessed May 5, 2020.
[8] Cybersecurity and Infrastructure Security Agency (CISA), the Election Assistance Commission (EAC), the Federal Bureau of Investigation (FBI), and the National Institute of Standards and Technology (NIST), "Risk Management for Electronic Ballot Delivery, Marking, and Return," May 2020.