MAIL-IN VOTING RISK:
INFRASTRUCTURE AND PROCESS

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, which build layers of safeguards to defend the process from manipulation.**
Implementation of mail-in voting infrastructure and processes within a compressed timeline may also introduce new risk.	Election officials 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 will build resiliency.
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.	Private sector partners are implementing technical and procedural best practices and sharing information through the EI-ISAC. USPS has a dedicated election mail program that includes an intelligent mail barcoding system enabling ballot tracking and chain of custody.
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.	Many jurisdictions have a cure process allowing voters correct a rejected ballot package. A voter who does not receive a ballot in the mail can go to a voting location and vote a provisional ballot.
The outbound and inbound processing of mail-in ballots introduces additional infrastructure and technology, increasing potential scalability of cyber attacks.	Compensating controls for additional infrastructure are the same as other election technology and infrastructure, so election officials should focus on cyber risk management best practices 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.	Some jurisdictions have implemented election technology and infrastructure to speed up the process. Some jurisdictions are legally afforded the opportunity to begin processing ballot application and ballots in advance of election day. Election officials, media, candidates, and NGOs are educating voters and setting the expectation that 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 NGOs are educating voters about the mail voting process. The National Association of Secretaries of State launched #TrustedInfo2020 to highlight state and local election officials as the credible, verified sources for election information.