This document is one in a series created as part of the Cybersecurity and Infrastructure Security Agency (CISA) Elections Infrastructure Government Coordinating Council and Sector Coordinating Council's Joint COVID Working Group. These documents provide guidance for state, local, tribal, and territorial election officials on how to administer and secure election infrastructure in light of the COVID-19 epidemic.

Electronic Ballot Delivery and Marking

Overview

In light of social distancing measures enacted in many areas of the country, many election officials are looking for ways to expand the options they can provide to their voters to cast a ballot privately and independently. One such option being considered is the expansion of electronic ballot delivery and marking.

Although there are risks associated with expanding the use of Internet-connected election technologies, election officials must manage those risks under the current conditions. This document provides a list of FAQs and considerations for jurisdictions intending to implement or expand the use of electronic ballot delivery systems.

Election officials typically have months or years to implement a new technology, but in the current environment, many do not have that luxury. Therefore, the Election Infrastructure Government Coordinating Council (GCC) and Sector Coordinating Council (SCC) are providing a list of considerations for election officials determining whether the expansion of electronic ballot delivery and marking is appropriate for their jurisdiction.

Policy and Legal Considerations[1]

Eligibility

- ❑ What laws or policies need to change?
    - ❑ Does your office have the authority to make changes without engaging lawmakers? Which, if any, stakeholders need to be engaged?
    - ❑ What is the relevant timeline that would apply to such lawmaker engagement? (e.g., when will the relevant legislative body be in session?)

[1] This document does not convey legal advice to any entity. Entities seeking legal advice should consult a lawyer.

- ❑ Who is currently eligible to receive an electronic ballot (i.e., Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) only, voters with disabilities, voters who did not receive mailed ballot, voters with an excuse, all voters, etc.)?
    - ❑ If you expand, to whom would you extend the option?
- ❑ How do eligible voters request a ballot or apply to receive an electronic ballot?
    - ❑ What information must the voter provide?
    - ❑ What format(s) will be available for the voter to apply (i.e., paper, online, fax, etc.)?
    - ❑ Will it apply to currently registered voters only, or will there be a way for voters to register electronically?

Ballot Transmission

- ❑ Do you have an online portal from which to download a ballot package?
    - ❑ Do you email a link or other notification to all eligible voters?
    - ❑ Do eligible voters need specific credentials to access the ballot package?
- ❑ Can you email the ballot package?
    - ❑ Do you send the ballot package as an attachment that must be downloaded?
    - ❑ Is the file in a fillable format (i.e., HTML, PDF, etc.) for the voter to digitally mark?
- ❑ Can you fax a copy of the ballot package?
- ❑ How do you confirm the receipt of the ballot?
- ❑ When is the last day a voter can request an electronic ballot?
- ❑ What is the last day the election official can transmit a ballot to the voter?

Voter Identification and Authorization Considerations

Voter File

- ❑ Is your current voter registration database capable of indicating that a voter has requested an electronic ballot?
- ❑ Will staff have to perform manual updates for every eligible voter who requests an electronic ballot or is there a way to do it in bulk?
- ❑ How will you handle voters who need a duplicate ballot (i.e., because of spoiled ballots, ballot was never received, etc.)?
- ❑ How will the voter file be annotated when the returned ballot is received?
- ❑ How will the voter file be updated to reflect the ballot being accepted?
- ❑ Can the voter check the status of their ballot?

Voter Credentials

- ❑ What credentials will a voter need to be able to access the electronic ballot (i.e., PII, biometrics, unique identifier, etc.)?
- ❑ How will the voter receive the necessary credentials to access his or her ballot (i.e., emailed from election official, mobile app, etc.)?
- ❑ How will voter credentials be secured?

System Considerations

Vendors

Many jurisdictions have opted to build their own system and others have purchased a system from an election technology vendor. The GCC does not endorse any specific vendor or product, thus you should speak with your colleagues on the GCC or in your state and/or consult election technology providers that have election technologies that meet the needs of your jurisdiction.

System Infrastructure

- ❑ How will the voting infrastructure be hosted (i.e., on servers at your facility, in the cloud, etc.)?
    - ❑ If you use the cloud, do you have awareness of where will the data be hosted (i.e. outside your jurisdiction, state, or the United States)?
- ❑ Does the system have the capacity to handle the increased load?
- ❑ What redundancies should be built into the system (i.e., backups, failover system, etc.)?
- ❑ Who will administer system configuration (i.e., security, load balancing, updates, patches, etc.)?

Electronic Interface

- ❑ Is the system accessible to voters with specific needs (i.e., visual impairments, disabilities, language, etc.)?
- ❑ Is the system compatible with mobile devices?
- ❑ Is the system compatible with readily available screen readers?
- ❑ Is the system accessible with binary personal assistive technologies (i.e., jelly switches, sip-n-puff, etc.)?
- ❑ Do you provide help to voters directly through the electronic ballot delivery system?

Ballot Definition Files

- ❑ What file format does your system accept (i.e., HTML, PDF, CSV, etc.)?

- ❑ Does your voting system produce ballots in the accepted file types, or do you need software to convert them?
- ❑ What type(s) of audio files does your system use?
- ❑ What languages do the ballots need to be presented in?

Additional Supplies

- ❑ Do you need to supply additional affidavits and instructions to the voter who votes electronically?
- ❑ Will your materials contain labels and self-folding envelopes to mail the ballots back?
- ❑ Will you provide printable privacy sleeves for the voter to protect the ballot?
- ❑ What auxiliary technologies are required for the voter to complete his or her ballot (i.e., Internet service, email, printer, fax service, specific software, etc.)?

Ballot Duplication

Many ballots generated by an electronic ballot delivery system cannot be directly scanned and tabulated into your voting system. To tabulate ballots using the voting system, the ballots must be printed on paper stock meeting certain specifications. For those ballots, enough blank paper stock will need to be purchased in advance. Jurisdictions may need additional technology (i.e., ballot duplication system, ballot on demand system, etc.) or staff to duplicate electronically generated ballots onto a ballot that can be scanned and duplicated. Depending on the volume of ballots that require duplication, additional staff needs could be significant.

Implementation Considerations

- ❑ When do you need to begin the implementation to meet your required timelines?
    - ❑ Is the timeline dependent upon your vendor?
- ❑ Will the vendor provide a dedicated point of contact for your jurisdiction?
- ❑ What training do your employees need?
- ❑ What additional central count equipment, storage space and training will be needed to tabulate the additional ballots?
- ❑ When do you need to begin voter education and outreach on the system?
- ❑ Who will provide technical assistance to voters (i.e., staff, vendor, etc.)?
    - ❑ How long will technical support be available to the voters (i.e., from the day ballots are sent, during early voting period, only election day, etc.)?
    - ❑ What times of day/days of the week will technical support be available?
    - ❑ How will voters receive technical assistance (phone, email, live chat, etc.)?
- ❑ Will the system's robustness be tested?
- ❑ Will you have the system's usability and accessibility for voters with disabilities tested?
- ❑ Will you have the system's security tested?

- ❑ NOTE: CISA can provide vulnerability (a.k.a. Cyber Hygiene) scanning, remote penetration testing, and other services at no cost to the jurisdiction and has conducted a critical product evaluation (CPE) on some vendor supplied systems.

Security Recommendations

Because these systems are publicly facing, jurisdictions using an electronic ballot delivery system should request a vulnerability scan and remote penetration test be conducted on the system. To request these services from CISA, email CISACustomerService@cisa.dhs.gov. Also, for vendor-provided systems, election officials should suggest that their vendor subject the system to a critical product evaluation. These services provide the situational awareness needed to make informed decisions to manage the risks associated with the system and are provided at no cost to election jurisdictions and their private sector partners. Furthermore, the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) has resources, guides, and tools available to election officials for protecting election infrastructure.

General

- ❑ Sign up for CISA services, such as vulnerability scans (aka CyHy), remote penetration testing (RPT), phishing campaign assessment, etc. All CISA services can be located in the CISA Election Infrastructure Security Resource Guide. All services can be requested at CISACustomerService@cisa.dhs.gov.
- ❑ Become an EI-ISAC Member by going to https://www.cisecurity.org/ei-isac/.
- ❑ All systems and technology used for the delivery of ballots should be separated from systems that are not required for the implementation of electronic ballot delivery.
- ❑ Best practices for securing voter registration data should be used to protect the personal identifying information from the voter registration database that is used to authenticate voters should use the data.

Fax

- ❑ Election officials should set up transmission reports when faxing a ballot package to the voter to verify that the ballot package was received by the fax machine to which it was sent.

Email

- ❑ Use a dedicated computer that is separated from the remainder of the election infrastructure. For very small offices that may not have the resources to use a dedicated computer, a virtual machine should be installed to separate these devices.

❑ Implement STARTTLS on your email servers to create a secure connection; this mainly provides confidentiality protection.
❑ Implement Domain-based Message Authentication, Reporting, and Conformance (DMARC), DomainKeys Identified Mail (DKIM), and Sender Policy Framework (SPF) on your emails to help authenticate the email you are sending the voter.
❑ Use a dedicated email address for receiving ballots, such as Ballots@County.Gov. Also, implement naming conventions that will help the voter recognize the email as legitimate (e.g., 2020 Presidential General).
❑ Implement two-factor authentication on all email systems used by election officials.
❑ Turn on read receipts so the election official can validate that the email ballot package was received.

Web-Based Portals and File Servers

❑ Use security best practices for web and network connected election systems, including two-factor authentication (2FA) for employees and voters.
❑ Encrypt traffic using secure hypertext transfer protocol (HTTPS) or, if you use a file server, ensure it uses a secure file transfer protocol (SFTP) by supporting transport layer security (TLS) version 1.2.
❑ Obtain outside cybersecurity assessments, such as CISA vulnerability scanning and remote penetration testing.

Resources

❑ CISA services can be located in the CISA Election Infrastructure Security Resource Guide. All services can be requested at CISACustomerService@cisa.dhs.gov.
❑ Become an EI-ISAC Member by going to https://www.cisecurity.org/ei-isac/.
❑ CISA's Binding Operational Directive (BOD)18-01 addresses enhancing email and web security
❑ NIST special publication (SP) 800-177 provides recommendations and guidelines for enhancing trust in email
❑ NIST SP 800-52r2 provides guidelines for selection, configuration, and use of TLS