ELECTRONIC BALLOT DELIVERY AND MARKING
Overview

- Military and Overseas Voters Empowerment Act requires all states to have the ability to transmit a digital copy of an unmarked ballot to the voter.
- Voters with specific needs, who want to vote by mail or absentee, benefit from similar functionality to vote from home.
- Remote Accessible Vote By Mail (RAVBM) is not monolithic, nor is it a technology.

* Some systems have additional capabilities that can introduce additional risks.

Three main components:
Ballot Delivery | Ballot Marking | Ballot Return
GCC-SCC Guidance on Delivery & Marking

Security Recommendations

Because these systems are publicly facing, jurisdictions using an electronic ballot delivery system should be a vulnerability scan and remote penetration testing conducted on the system. To request these services from CISA, email CISAGovSecurity@uscit.gov. Also, for vendor-provided systems, election officials should sign that they have tested the system to a critical path 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 (EIISC) has resources, guides, and tools available to election officials for protecting election infrastructure.

General
- Sign up for CISA services, such as vulnerability scans (aka Cyber), remote penetration testing (RPT), phishing campaign assessment, etc. All CISA services can be located at CISA/GovSecurity/Election Security.
- Become an EIISC Member by going to https://www.security.uscis.gov.
- 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.

Fax
- Election officials should set up transmission reports when faxing a ballot package to the verifier 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.

Considerations on:
- Policy and Legal
- Voter Identification and Authorization
- System(s)
- Implementation

Security Recommendations

Resources

Developed in 2020 by GCC-SCC
Joint COVID Working Group
Risk Management Guidance

Risk Management for Electronic Ballot Delivery, Marking, and Return (FOUO):

- EAC, NIST, FBI, and CISA assessed and compared risk for three processes
- Identified technologies and systems used
- Issued technical best practices for risk management
Ryan Macias
SME Consultant, CISA

electionsecurity@hq.dhs.gov

Contact CISA:
Central@cisadhs.gov