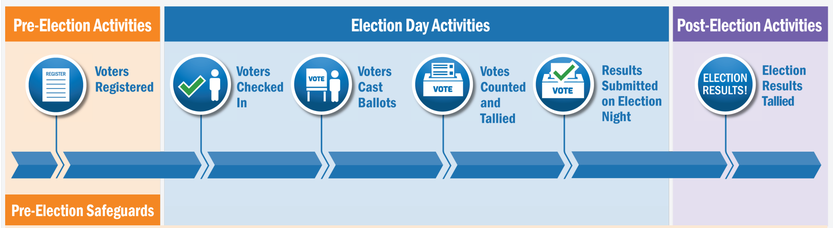
2018 Election Cybersecurity Planning Snapshot

State of Maryland

SAFEGUARDS / RESILIENCY MEASURES

Maryland Election Process



Pre-Election Safeguards

Voters Registered

- Voter registration database security measures include rigorous monitoring, a multi-layer defense, and regular security updates.
- All State and local election officials receive regular security training and work with DHS to ensure the database meets federal security standards.
- Integrity of the voter registration database verified through all authorized sources.

Election Day Safeguards

Voters Checked In

- Poll worker verifies voter identity by matching voter's ID to voter database.
- Electronic pollbooks are provided at all voting locations.
- Failsafe measures protect voter's right to vote.

Voting, Tallying, & Reporting Systems

- Vigorous logic and accuracy testing before election.
- Voting systems are never connected to the internet.
- Ballots are securely stored with extensive chain of custody procedures.

Voters Cast Ballots

- Maryland's elections are paper ballot-based with electronic tabulation; the paper ballot is the official record.
- Absentee ballots must be returned by mail or delivered in person; electronic submission is prohibited.
- Absentee ballots tracked and kept in a secure location.

Post-Election Safeguards

Election Results Tallied

- Precinct and state officials compare and reconcile the number of ballots with the number of voters who signed in at the polling place.
- Post-election audits include an independent, 100% tabulation of ballot images before certifying official election results; audit results are available to the public.

Election Day Security Guidelines

Ballot security: All marked paper ballots are scanned, tabulated, and secured in a locked ballot box. After polls close, the local boards of elections will safely store the marked paper ballots.

Equipment security: Election officials test each ballot scanner before each election. After testing, election officials seal each ballot scanner and store it in a secure location until it is securely moved to a voting location. Each scanner is sealed until it is ready to use.

THREAT MITIGATION

Specific Threats / Mitigation

Social Engineering refers to bad actors who manipulate their target into performing a given action or divulging certain information (often a login or password). "Spear-phishing" (sending an email attachment or link to infect a device) is the most common. ***Mitigation:*** Education and training on threats and types of targeted information; conducting phishing campaign assessment

Information Operations include propaganda, disinformation, etc., to manipulate public perception. Methods include leaking stolen information, spreading false information, amplifying divisive content, and/or interrupting service. ***Mitigation:*** Clear and consistent information, including accurate cybersecurity terminology; relationship building with the media; open dialog with the public

Hacking refers to attacks that exploit or manipulate a target system to disrupt or gain unauthorized access. ***Mitigation:*** Incident response and recovery planning; penetration testing; strong passwords and two-factor authentication, especially for admin access; encrypted password storage and transmission; active system monitoring; current security updates; upgrades to supported OS and applications; physical security

Distributed Denial of Service (DDoS) attacks seek to prevent legitimate users from accessing information (e.g., databases, websites) or services by disrupting access with excessive traffic, causing the service to crash. ***Mitigation:*** Business continuity and incident response planning; anti-virus software and firewall; good security practices for distributing your email address; email filters

Insider Threat is a category of attack in which a current or former employee or authorized individual with access to a network, system, or data deliberately uses their access for malicious purposes. ***Mitigation:*** Background checks for all election workers and contractors; insider threat training; vigorous chain-of-custody records; strict access controls based on need and updated as access needs change

Definitions from The State and Local Election Cybersecurity Playbook / Defending Digital Democracy (www.belfercenter.org/D3P)

Recognizing and Reporting an Incident

Definition of an Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices (NIST Pub. 800-61)

If you suspect a Cybersecurity Incident has occurred, contact—

- Maryland State Board of Elections, (410) 269-2840, (800) 222-8683 (Toll Free), (800) 735-2258 (TTY), or info.sbe@maryland.gov
- National Cybersecurity and Communications Integration Center (NCCIC), (888) 282-0870 or NCCIC@hq.dhs.gov
- Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) Security Operation Center, (866) 787-4722 or soc@cisecurity.org

For Additional Information or Questions

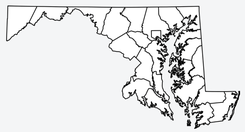
Maryland State Board of Elections: (410) 269-2840, (800) 222-8683 (Toll Free), (800) 735-2258 (TTY), or info.sbe@maryland.gov

U.S. Department of Homeland Security: www.dhs.gov/topic/election-security

- Franco Cappa, Region III Cybersecurity Advisor, franco.cappa@hq.dhs.gov
- William J. Ryan, Region III Director for Infrastructure Protection, ipregion3ops@hq.dhs.gov

2018 ELECTION INITIATIVES

State Election Data



Precincts: 1,991
Active Voters: 3,955,316 (as of September 2018)
Optical Voting System: ES&S DS 200 Scanning Unit
Accessible System: ES&S Express Vote Ballot Marking Device
Website: elections.maryland.gov

2018 Activities and Timeline Checklist

- [x] **Initiative 1:** Schedule Cyber Hygiene Scanning. Contact ncciccustomerservice@hq.dhs.gov and reference "Maryland Cyber Hygiene Initiative" to obtain this service free through DHS *(Completed October 2016)*
- [x] **Initiative 2:** Conduct Regional Manager Computer Assessments – monthly assessment of all computers accessing Election Systems. *(Coducted monthly starting in April 2017)*
- [x] **Initiative 3:** Conduct a Phishing Campaign Assessment. Contact ncciccustomerservice@hq.dhs.gov and reference "Maryland Phishing Campaign Assessment" to obtain this service free through DHS *(Completed March 2018)*
- [x] **Initiative 4:** Install Albert Sensor to continuously monitor network traffic for critical election systems. *(Completed May 2018)*
- [x] **Initiative 4:** Register for the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) at learn.cisecurity.org/ei-isac-registration *(Completed July 2018)*
- [x] **Initiative 5:** Hold Statewide Table Top Training exercise with Local Boards of Election. *(Completed August 2018)*
- [ ] **Initiative 7:** Implement two-factor authentication requirement for users to access voter registration database *(Target Completion: October 2018)*

Revised as of October 1, 2018

Developed by the Maryland State Board of Elections
w/ support from the US Department of Homeland Security – Election Task Force