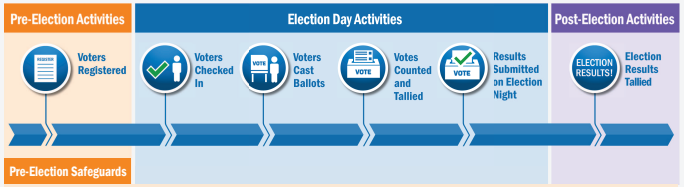
SOUTH CAROLINA ELECTION COMMISSION

2018 Election Cybersecurity Planning Snapshot
South Carolina

SAFEGUARDS / RESILIENCY MEASURES

South Carolina Election Process



Pre-Election Safeguards

Voters Registered

- Voter registration system is protected by firewalls and monitored 24/7 for intrusions
- System is accessed through user IDs, passwords, and two-factor authentication
- Users receive security training and follow strict security policies and procedures

Election Day Safeguards

Voters Checked In

- Voters present Photo ID
- Voters located on voter registration list and asked to verify address
- Failsafe measures protect voter's right to vote

Voters Cast Ballots

- Voting machines are kept secure and are arranged so that the voter can cast his or her ballot without crowding, confusion, or interference

Voting, Tallying, & Reporting Systems

- Security protocols are formalized in policy and procedure
- Vigorous logic and accuracy testing is conducted before each election and is open to the public
- Voting machines are not connected to the internet
- Voting machines and paper ballots are securely stored with extensive chain of custody records
- Cyber and physical security measures ensure voting system integrity on election day

Post-Election Safeguards

Election Results Tallied

- Results are unofficial until the canvass of votes
- Canvass compares printed report from precincts to number of voters signed in on poll list
- Vigorous chain of custody records maintained
- Results from voting machines are verified against audit logs for accuracy prior to certification
- Post-election audit performed on all precincts

Election Day Security Guidelines

From South Carolina Election Official Manual

Polling Place Security: Poll managers must maintain custody of voting machines, ballots, the communications pack, the EVRL laptop, the paper voter registration list and other election materials to and from the polling place. Poll managers maintain control at the polling place to ensure a safe and orderly voting process

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 and 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 planning, penetration testing, two-factor authentication, recovery planning active system monitoring and current security updates along with physical security measures

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—

- State Election Commission and/or your county IT manager
- 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

In the event of a Data Breach impacting more than 1000 people, notify—

- South Carolina Department of Consumer Affairs, Identify Theft Unit, (803) 734-4200 or scdca@scconsumer.gov

For Additional Information or Questions

State Election Commission: elections@elections.sc.gov

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

- Klint Walker, Region IV Cybersecurity Advisor, klint.walker@hq.dhs.gov
- Donald Robinson, Region IV Director for Infrastructure Protection, ipregion4outreach@hq.dhs.gov

2018 ELECTION INITIATIVES

Election Data

Precincts: 2,245 (as of July 2018)

Active Voters: 3,054,327 (as of July 2018)

Voting Systems: Electronic voting machines are used at polling places. Optical scan ballots are used for voting absentee by mail

Website: scVOTES.org

Phone: (803) 734-9060

2018 Activities & Timeline Checklist

- **Initiative 1:** State participates in DHS cyber hygiene scanning program. *(Target Completion: Ongoing)*
- **Initiative 2:** Harden security of voting system through use of secure endpoints, encrypted media, and standardized, single-purpose election management workstations. *(Target Completion: June 1)*
- **Initiative 3:** Participate in two-day security workshop and table-top exercise with federal and state security partners. *(Target Completion: August 8)*
- **Initiative 4:** Register for the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) at learn.cisecurity.org/ei-isac-registration *(Target Completion: September 1)*
- **Initiative 5:** Complete biannual, state mandated, system end-user cybersecurity training. *(Target Completion: Ongoing)*
- **Initiative 6:** State conducts phishing campaign assessments for all system users. *(Target Completion: Ongoing)*
- **Initiative 7:** Participate in DHS physical security assessments of state and county facilities. *(Target Completion: October 31)*

Revised as of August 3, 2018

DEVELOPED BY THE S.C. STATE ELECTION COMMISSION

W/ SUPPORT FROM THE US DEPARTMENT OF HOMELAND SECURITY – ELECTION TASK FORCE

EVERY VOTE MATTERS. EVERY VOTE COUNTS.