# 2018 Election Cybersecurity Planning Snapshot

## Anderson County

### South Carolina Election Process

**Pre-Election Activities**
- Voters Registered
- Voters Checked In
- Voter ID

**Election Day Activities**

**Post-Election Activities**
- Election Results Tallied
- Results Asserted on Election Night
- Results Certified on Election Day

### Election Day 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

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

**Voters Cast Ballots**
- Paper ballots are securely stored with an extensive chain of custody records
- Voting machines are kept secure and are arranged so that the voter can cast his or her ballot without crowding, confusion, or interference

**Results Tallied**
- Results are uncounted until the canvass of votes is complete
- 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:**
  - Vigorous chain of custody records maintained
  - Number of voters signed in on poll list
  - Canvass compares printed report from precincts to
  - Voting machines are not connected to the internet
  - Vigorous logic and accuracy testing is conducted before

- **Poll managers must maintain custody of voting machines, ballots, the communications pack, the**
  - System integrity on election day
  - Defend from hacking
  - System end-user cybersecurity training.

### 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)
- "Phishing" (sending an email attachment or link to infect a device) is the most common.

**Information Operations**
- Use propaganda, disinformation, etc., to manipulate public perception.
- Methods include leaking stolen information, spreading false information, amplifying divisive content, and/or interrupting service.

**Hacking**
- Refers to attacks that exploit or manipulate a target system to disrupt or gain unauthorized access.

**Insider Threat**
- A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices

#### 2018 Election Initiatives

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

### 2018 Activities & Timeline Checklist

- **Pre-election initiatives**
  - **Initiative 1:** Participate in two-day security workshop and tabletop exercise with federal and state security partners. (Target Completion: August 8)
  - **Initiative 2:** Harden security of voting system through use of secure endpoints, encrypted media, and standardization, single-purpose election management workstations. (Target Completion: June 1)
  - **Initiative 3:** Participate in two-day security workshop and tabletop 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)

---

**Anderson County Overview**

- **Precincts:** 80 (as of July 2018)
- **Active Voters:** 114,270 (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:** (864) 260-4035

---

**For Additional Information or Questions**

- **State Election Commission:** elections@elections.sc.gov
  - Klint Walker, Region IV Cybersecurity Advisor, klint.walker@hq.dhs.gov
  - Donald Robinson, Region IV Director for Infrastructure Protection, donald.robinson@hq.dhs.gov
  - National Cybersecurity and Communications Integration Center (NCCIC), (888) 282-0870 or nccic@dhs.gov
  - Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), (866) 767-4722 or ei-isac@cisecurity.org
  - Information Sharing and Analysis Center (EI-ISAC) at learn.cisecurity.org/ei-isac-registration

---

**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

**Definition of an Incident:**
- State Election Commission and/or your county IT manager
- National Cybersecurity and Communications Integration Center (NCCIC), (888) 282-0870 or nccic@dhs.gov
- Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), (866) 767-4722 or ei-isac@cisecurity.org
- In the event of a Data Breach impacting more than 1000 people, notify—
  - Anderson County
  - South Carolina Department of Consumer Affairs, Identity Theft Unit, (803) 734-4200 or identity@sc.gov

**For Additional Information or Questions**

- **State Election Commission:** elections@elections.sc.gov
  - Klint Walker, Region IV Cybersecurity Advisor, klint.walker@hq.dhs.gov
  - Donald Robinson, Region IV Director for Infrastructure Protection, donald.robinson@hq.dhs.gov
  - National Cybersecurity and Communications Integration Center (NCCIC), (888) 282-0870 or nccic@dhs.gov
  - Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), (866) 767-4722 or ei-isac@cisecurity.org

---

**Developed by the S.C. State Election Commission**

**COVID-19**

**Support from the U.S. Department of Homeland Security — Election Task Force**

---

**SAFEGUARDS / RESILIENCY MEASURES**

### Election Day Security Guidelines

- **Polling Place Security:** Poll managers maintain custody of voting machines, ballots, the communications pack, the EVR 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.

---

**SAFEGUARDS / RESILIENCY MEASURES**

### Election Day Security Guidelines

- **Polling Place Security:** Poll managers maintain custody of voting machines, ballots, the communications pack, the EVR 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.