SOUTH CAROLINA
ELECTION COMMISSION

Securing South Carolina Elections

August 21, 2018

Our Top Priority

The mission of the S.C. State Election Commission (SEC) is to ensure every eligible citizen has the opportunity to register to vote, participate in fair and impartial elections, and have the assurance that their votes will count. Fundamental to this mission is ensuring the security and integrity of elections in South Carolina. Elections face numerous threats from a wide variety of actors including nation states, individuals and organizations – all with various motives. We recognize these threats, and we want voters to know we have made it our top priority to take all reasonable measures to improve and protect the security and resilience of our state's election infrastructure.

Our Security Team

To address these threats against critical infrastructure, the SEC has developed an unprecedented security partnership of state, federal and private cybersecurity professionals as well as state and federal law enforcement and intelligence agencies.

The U.S. Department of Homeland Security (DHS) provides a multitude of resources and services including cyber hygiene scanning, risk and vulnerability assessments, and security training. DHS also provides communication and collaboration through information sharing, alerts, in-person support from cybersecurity and physical security advisors, and incident response services.

The S.C. Department of Administration, Division of Technology houses and secures the state's voter registration system. The Division of Technology manages, monitors, and performs vulnerability scans for the statewide voter registration system and agency networks.

We have also partnered with a private cybersecurity firm to provide risk and vulnerability assessment, management and remediation, as well as advice on strengthening our security posture.

In addition, the State Law Enforcement Division (SLED), the Federal Bureau of Investigation (FBI), and the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) provide information sharing and incident prevention and response support.

Our Approach

We are taking numerous actions that include installing and reconfiguring equipment and software, revising policies and procedures, and improving and expanding training and awareness initiatives. These actions are designed to ensure a strong and resilient election infrastructure that will continue to serve citizens in the face of any adversity.

- Network Based Security – Networks are protected against threats using various tools and concepts including firewalls, intrusion prevention and detection systems, network sensors, 24/7 monitoring, data encryption, incident reporting mechanisms, software application patch management, two-factor user authentication, user password strength requirements, and user password expiration.
- Risk and Vulnerability Assessments – Cyber and physical security assessments and penetration tests are performed to identify any vulnerabilities. All vulnerabilities, regardless of severity, are addressed immediately.
- Training and Education – We work to establish a strong security culture by training election officials to follow security policies and procedures and to recognize cyber threats and attack methods including identifying phishing emails and other social engineering attacks. Users are required to complete cyber security training before being granted access to systems and on an ongoing basis to maintain access. The SEC conducts field audits to ensure election officials are following security policies and procedures.
- Voting System Security – Before being used in a South Carolina election, the voting system was tested and certified by a testing laboratory approved by the U.S. Election Assistance Commission (EAC) and was tested by the SEC to ensure the system met the requirements of state law. Logic and accuracy tests are performed before every election to ensure the system is tallying votes correctly. Voting machines and the computers used to tabulate results are never connected to the internet. Voting system security plans and procedures are in place to insulate the system from unauthorized access including secure storage, access logs, data encryption, and data transfer through secure endpoints. Election results are tallied and reported publicly at the precinct-level, then at the county and state levels providing multiple checkpoints in the process. Post-election audits of all voting system data are conducted prior to certification of an election.

Securing Future Elections

Security is a never-ending process. We remain vigilant as the election environment changes and new threats emerge. We must rise to meet those threats by establishing new layers of security to further build the resilience of our state's election infrastructure.

South Carolina's current voting system was implemented in 2004 and is reaching the end of its expected useful life of 15 years. While we take significant measures to secure the system and are confident it will meet the needs of voters in 2018, we are planning for the transition to a new voting system by 2020. The SEC continues working with the S.C. General Assembly to acquire funding for this replacement effort.

Replacement will not only provide the state with a dependable system that will serve voters for years to come but will improve the security and resilience of our election process. In line with our approach of taking all reasonable measures to secure the state's election infrastructure, any

new system will have a paper record of each voter's voted ballot. This will add an important layer of security as it allows for audits of hand-counted ballots to verify vote totals.

Considering the significant efforts being made to secure our elections, we want you to go to the polls and vote with confidence knowing your vote matters, and your vote will count. Our democracy depends on it.