SECURING YOUR VOTE

R. KYLE ARDOIN
SECRETARY OF STATE

THE LOUISIANA ELECTION PROCESS

BEFORE THE ELECTION

- Roughly 10,000 voting machines are owned and warehoused by the Secretary of State's Office.
- All voting machines are thoroughly serviced before each election.
- No voting machine is ever connected to a network or the internet.
- All voting machines are publicly tested and sealed prior to each election.

DURING THE ELECTION

- Electronic and physical security measures ensure the integrity of all voting systems used for voting absentee-by-mail, during early voting, and on Election Day.
- Uniform statewide protocols are included in formalized policy.
- Only trained and certified commissioners and Secretary of State voting machine technicians operate the voting equipment allowing voters to cast their votes.
- Paper ballots (used for absentee-by-mail voting, provisional voting for federal elections, and during emergencies) are tracked and securely stored.
- Voters must present ID or have their identity and eligibility confirmed by the Registrar of Voters to ensure that only eligible voters are allowed to cast a vote.

AFTER THE ELECTION

- Results are unofficial until audited, compiled, and promulgated.
- The Secretary of State's audit process compares signatures in the precinct register to the number of voters at the polls and ballots cast. This is done statewide prior to certifying results as official.

The **SECRETARY OF STATE** is the chief election official of the State of Louisiana. He administers the laws relating to custody of voting machines and voter registration.

The **STATE BOARD OF ELECTION SUPERVISORS** reviews election laws and procedures, conducts hearings for complaints made under federal election laws, and conducts appeals of merit evaluations of Registrars of Voters.

The **REGISTRARS OF VOTERS** are responsible for registering eligible voters, maintaining voter registration records, and conducting early voting in their parish.

The **CLERKS OF COURT** are the chief election officers of their parish and the ex officio parish custodians of voting machines. They are responsible for training and certifying commissioners and transmitting results to the Secretary of State's Office on election night.

The **PARISH BOARDS OF ELECTION SUPERVISORS** supervise the preparation for and conduct of all elections held in their parish. They select commissioners, accept and count absentee-by-mail ballots, and accept and count provisional ballots for federal elections.

CYBERSECURITY THREATS AND MITIGATION

THREAT: 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:** Cyber hygiene training, which includes securing the human training.

THREAT: 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.

THREAT: 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.

THREAT: 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 email addresses, and email filters.

THREAT: 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, insider threat training, vigorous chain-of-custody records, strict access controls based on need, and updating 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 or other security incident has occurred, contact the Louisiana Secretary of State's Office at 800.883.2805 or admin@sos.la.gov.

This public document was published at a total cost of $1,071.54. 8,550 copies of this public document were published in this first printing at a cost of $1,071.54. The total cost of all printings of this document, including reprints is $1,071.54. This document was published by the Louisiana Department of State for educational purposes under authority of a special exemption by the Division of Administration. This material was printed in accordance with the standards for printing by state agencies established pursuant to R.S. 43:31.