SECURING YOUR VOTE

Nancy Landry
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. (Only Secretary of State, Registrar of Voters, or Clerk of Courts personnel store, program, or operate the voting equipment.)
- All voting machines are thoroughly serviced before each election.
- No voting machine is ever connected to the internet.
- All voting machines are publicly tested and sealed with tamper evident seals prior to each election during the PBES verification, test, and seal process.

DURING THE ELECTION

- Electronic and physical security measures ensure the integrity of all voting systems used for absentee voting, during early voting, and on Election Day.
- Statewide protocols are included in formalized policy to ensure uniform procedures and that only one ballot per person is cast.
- Only trained and certified commissioners and Secretary of State voting machine technicians operate the voting equipment.
- Paper ballots (used for absentee 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's Election Compliance Unit investigates all reported voting irregularities.

STATE ELECTION OFFICIALS

The **SECRETARY OF STATE** is the chief election official of the State of Louisiana and administers the laws relating to custody of voting machines and voter registration and is responsible for securing election information. In addition, the Secretary of State provides every parish with support staff during early voting and on election night.

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 parishes and the ex officio parish custodians of the 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 (PBES)** are bipartisan boards that supervise the preparation for and conduct of all elections held in their parishes. They select commissioners, accept and count absentee ballots, and accept and count provisional ballots for federal elections.

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.

CYBERSECURITY THREATS AND MITIGATION

THREAT: SOCIAL ENGINEERING is usually a low-tech attack that attempts to trick users into providing information that can be used to compromise the security of a system. The most common form of social engineering attacks include "phishing" or "vishing", which are attacks through fake emails or phone calls. **MITIGATION:** Cyber hygiene, multi-factor authentication, and cybersecurity training for the workforce.

THREAT: DISINFORMATION AND MISINFORMATION CAMPAIGNS are information operations that attempt to manipulate public opinion and/or influence behavior with false or misrepresented information. These campaigns typically are low-cost and spread rapidly with digital technologies such as social media, email, or fake websites. **MITIGATION:** Promote transparency, get involved, and verify information about elections directly from trusted sources such as the Secretary of State, your local Registrar of Voters, or Clerk of Court.

THREAT: HACKING is a general term that refers to many types of attacks focused on exploiting or manipulating a target system to disrupt or gain unauthorized access. **MITIGATION:** Follow security best practices, have an incident response plan, proactively test for vulnerabilities, keep systems properly updated, train the workforce, and implement proper security measures.

THREAT: DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACKS seek to prevent legitimate users from accessing information or services by flooding the service with excessive traffic in an attempt to crash the service, which causes it to become temporarily unusable. **MITIGATION:** Implement and test business continuity plan and incident response plan, follow security best practices for preventing a DDoS attack, and proactively monitor systems to stay ahead of an attack.

THREAT: INSIDER THREAT is a category of attack in which an authorized individual with access to a network, system, or data knowingly or unknowingly leaks confidential data, allows unauthorized access, or manipulates a system. **MITIGATION:** Background checks, separation of duties, checks and balances, insider threat training, strict access controls, and Data Loss Prevention (DLP) solutions.

THREAT: SOCIAL MEDIA ACCOUNT COMPROMISE refers to bad actors, foreign and domestic, using social engineering attacks to learn usernames and passwords of social media accounts. Bad actors then utilize the stolen credentials to launch disinformation or misinformation campaigns from the compromised social media account. **MITIGATION:** Utilize strong passwords, enable multi-factor authentication when available, and identify points of contact with social media platform representatives (e.g. Facebook, Twitter, etc.).

THREAT: FAKE SOCIAL MEDIA ACCOUNTS are created by malicious actors, foreign and domestic, in an attempt to trick the public into believing they are an official source of information. These fake accounts are then used to launch disinformation and misinformation campaigns. **MITIGATION:** Verify information about elections directly from trusted sources such as the Secretary of State, your local Registrar of Voters, or Clerk of Court, report possible fake accounts to the proper platform (e.g. Facebook, Twitter, etc.), and check that the social media account has been verified by the platform.

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.

SYV - NL (Rev. 1/24)