CALIFORNIA SECRETARY OF STATE

ELECTION CYBERSECURITY

Office of Election Cybersecurity

Website: Cybersecurity.sos.ca.gov

Safeguarding our Elections

Fair and accurate elections are the bedrock of our democracy. The Secretary of State's Office collaborates with multiple government agencies to ensure that Californians can vote with confidence.

Together, we are protecting the integrity of our elections, safeguarding against potential cyberattacks, and ensuring that every vote is counted. Here is how we are safeguarding our state's elections:

Investing in New Systems:

- The Secretary of State's office has administered over$221 million dollars in state funding for voting infrastructure updates, including strengthening the accessibility, accuracy, security, and safety of our elections.

- In addition, California has been awarded and distributed over $73.5 million dollars in federal funding from the U. S. Election Assistance Commission (EAC), between 2018 and 2022 for election security.

Protecting Election Infrastructure

- California has one of the most strenuous voting system testing and certification programs in the country. Any new voting systems in California must receive certification and undergo months of testing, including functional testing, source code review, red team security testing that involves experts trying to "break into" the voting system, and accessibility and volume testing.

- California mandated that every ballot must either be paper or have a voter verifiable paper audit trail.

- Elections officials conduct a manual audit of a random 1% of ballots to ensure vote count machines are accurate.

- In collaboration with the California Office of Emergency Services, the Secretary of State's Office has launched the California Election Security Task Force to ensure local officials have robust support from state and federal infrastructure security partners in case of a security incident.

Office of Election Cybersecurity and Office of Risk Management

- The California Legislature appropriated an unprecedented $3 million to combat misinformation and strengthen cybersecurity by establishing The Offices of Election Cybersecurity (OEC) and Office of Risk Management (ORM) within the Secretary of State.

- Our Communications Department develops election information-correction campaigns, improves outreach to communities in rural and urban areas, and assists county elections officials and voters with up-to-date information about potential threats.

- The Office of Election Cybersecurity coordinates efforts between the Secretary of State and local elections officials to expand cyber-attack prevention capabilities and establish improved cyber incident response.

- The Office of Risk Management implements infrastructure security measures to protect the Secretary of State.

Partnering with Federal and Local Partners

- We continually work with federal, state, and local partners—including The Department of Homeland Security, The Federal Bureau of Investigation, CA Department of Technology, CA Office of Emergency Services, California Highway Patrol, and county elections officials—to share election security information and best practices.

- Our office hosts cybersecurity trainings with our federal and state partners, as well as organizing tabletop exercises and drills for county elections officials.

Be an Informed Voter and Report Suspected Misinformation.

- Be vigilant about the election information you consume and share on social media.

- Make sure that you receive your elections information from official sources such as local county elections officials and the California Secretary of State's office.

- If you suspect election information on social media is false or misleading, report it to your social media network and contact the California Secretary of State's office by emailing VoteSure@sos.ca.gov.