BRENNAN CENTER FOR JUSTICE

California

Top 5 Actions to Strengthen Election Security

American elections face an evolving landscape of security threats, from bomb threats and physical attacks on election infrastructure to cyberattacks and harassment of election workers. The 2024 election cycle saw hundreds of security incidents targeting polling locations, election offices, and ballot drop boxes, with many threats appearing to originate from foreign adversaries.

While coordinated state and local responses demonstrated effective ways to prevent and mitigate these threats, the federal government has significantly reduced its support for election security, undermining its role as a hub for coordination and communication. The current administration has frozen key cybersecurity programs, cut personnel, ended funding for information-sharing networks, and sought access to sensitive election systems and data.

Against these challenges, it is critical for states to take the lead in protecting election security and safeguarding American democracy.

Recommendations:

1. **The State Legislature should improve state law to better protect voting systems from unauthorized access.** Current state law prohibits (1) damaging, tampering with, or interfering with (or attempting) the correct operation of a voting system; and (2) interfering with or attempting to interfere with the secrecy of voting software. The latter includes breaking the chain of custody and possessing credentials or passwords, without authorization. Cal. Elec. Code § 18564. Furthermore, state law requires election officials to notify the Secretary of State whenever the chain of custody of a voting system (or component) has been compromised or the security has been breached. Cal. Elec. Code § 17603.

   To strengthen these protections, the state legislature should:

   - Provide a clearer definition of what constitutes "authorization," for example by including a specific list of individuals with authority to access voting systems.
   - Require election officials to notify the state election office whenever any third party requests access to voting systems, regardless of whether there is evidence of breach.

2. **The Secretary of State should update regulations and guidance on access to voting systems and election technology.** With or without additional legislation, the Secretary of State should issue regulations and guidance to clarify the meaning of "unauthorized" access and what constitutes an attempted "breach" triggering the requirement to notify the Secretary of State. The Secretary of State can enact these regulations pursuant to the office's power to "adopt regulations governing the use of voting machines, voting devices, vote tabulating devices, and ballot marking systems." Cal. Elec. Code § 19100.

   The Secretary can further protect election systems by requiring multi-factor authentication for all critical systems, including election management systems and e-pollbooks.

3. **The State Legislature should provide reliable funding for election infrastructure, ensuring that election officials can upgrade outdated hardware, secure technology, and keep facilities safe.** To protect election infrastructure against evolving cyber and physical security threats, the legislature can:

    - Establish a revolving fund to help election officials replace outdated voting systems and other technology as new systems built to modern standards become available;
    - Provide funding to ensure that counties can continue to access essential cybersecurity services that the federal government no longer funds through MS-ISAC, including protective DNS, phishing assessments, multifactor authentication, endpoint detection, and vulnerability scanning; and
    - Provide funding for election officials to address vulnerabilities identified through recent physical security assessments of election facilities.

4. **The Governor should direct state agency leaders to identify opportunities for election security support and collaborate with the Secretary of State's office to deliver support to local officials.** As the federal government cuts or deprioritizes support for cyber and physical security assessments, trainings, and incident response support, California should explore how to replace this support and expertise at the state level.

    The Governor should:

    - Direct leaders of relevant state agencies, including state IT, emergency management, homeland security, and law enforcement agencies, to assess internal resources and capacity available to assist election officials.
    - Utilize and strengthen the Office of Emergency Services' Election Security Task force to coordinate with the Secretary of State and deliver support to county officials.

5. **The Attorney General should educate election officials and law enforcement on laws governing threats to election workers and interference with election systems and processes.** The Attorney General and other state law enforcement officials should:

    - Reach out to and educate law enforcement officers on election law and administration, since most officers have limited familiarity with these areas due to infrequent high-turnout elections and rare incidents. Distribute reference guides.
    - Distribute handbooks that summarize relevant federal and state law, including prohibitions on voter intimidation, interference, and equipment tampering.
    - Work with the Secretary of State to ensure county election officials understand their requirements under federal and state law to protect election systems and voter data.

For more recommendations to secure elections, see the Brennan Center's recent report:
A State Agenda for Election Security and Resiliency