BRENNAN CENTER FOR JUSTICE

Securing the 2024 Election

PUBLISHED APRIL 27, 2023

U.S. elections face serious threats to their security and integrity, both from foreign adversaries and domestic actors seeking to undermine confidence in the democratic process. These threats have evolved and expanded in recent years to include disinformation campaigns, harassment and intimidation of election workers, insider attacks from within election offices, and cyberattacks. Ahead of the 2024 election, policymakers at all levels of government must work together to address these overlapping threats and strengthen the resiliency of the U.S. election system. This will require increased resources from federal agencies such as the Department of Homeland Security (DHS) and its Cybersecurity and Infrastructure Security Agency (CISA), the Department of Justice (DOJ), and the Election Assistance Commission (EAC); new laws to protect election workers and prevent insider attacks; and the expansion of ongoing efforts by state and local officials to preempt false information, including falsehoods generated by artificial intelligence (AI), and prepare for cyberattacks.

Read the full report here.

Key Recommendations for the Federal Government, State Legislatures, and State and Local Election Officials

THREATS	FEDERAL GOVERNMENT	STATE LEGISLATURES	STATE AND LOCAL ELECTION OFFICIALS
Spread of false information	■ CISA should share best practices for strengthening societal resilience to the spread of false election information — including falsehoods generated by AI — and promote the dissemination of accurate information from election officials, including through public-private partnerships. ■ CISA should escalate efforts to help local officials adopt and transition to .gov domains for election websites. ■ The EAC, working with CISA, should build public awareness and confidence in voting system security.	■ Mandate that local election offices use .gov domains. ■ Prohibit the spread of materially false information concerning the time, place, or manner of voting with the intent to prevent voters from exercising their right to vote. ■ Allow earlier processing and counting of mail ballots.	■ Dedicate resources to anticipate and refute false election information through public outreach.

Continued on next page

Continued from previous page

THREATS	FEDERAL GOVERNMENT	STATE LEGISLATURES	STATE AND LOCAL ELECTION OFFICIALS
Harassment and threats of physical violence	■ CISA should increase resources to protect election workers and sites, including by establishing regional election leads and increasing the number of protective security advisers (PSAs). ■ DHS should continue to require states to spend a portion of homeland security grants on election security, as it did in 2023. ■ DOJ's election threats task force should expand coordination with local election officials and law enforcement and reduce barriers for reporting threats.	■ Fund physical security protections and training. ■ Allow election workers to protect personally identifiable information. ■ Prohibit intimidation and doxing of election workers and ensure that all workers receive protection throughout the entire election process.	■ Direct federal grant funding to physical security needs. ■ Improve election workers' access to address confidentiality programs. ■ Provide training on protecting personal information.
Insider threats	■ CISA should expand its insider threat services by creating additional best practice checklists, developing self-assessment tools, and training PSAs on these materials.	■ Limit access to critical election infrastructure to officials and others needed to ensure that those systems function. ■ Establish authority to prohibit individuals who violate election laws from administering elections and to decommission jeopardized equipment. ■ Require election officials to use voting machines for initial ballot counts in all but the smallest jurisdictions, followed by bipartisan hand-count audits.	■ Develop regulations, protocols, and training to prevent, detect, and respond to insider attacks.
Cyberattacks	■ DHS should ensure that a portion of State and Local Cybersecurity Grant Program funding is set aside for election security. ■ CISA should increase resources to protect election systems, including by establishing regional election leads and hiring additional cybersecurity advisers (CSAs). ■ DHS, DOJ, CISA, and the EAC should educate election officials on federal grant opportunities and help direct funding to the areas of greatest need.	■ Fund the replacement of outdated election systems. ■ Mandate robust postelection audits. ■ Launch cyber navigator programs to help local jurisdictions defend against cyberattacks.	■ Adopt backup systems that allow voting to continue in the event of technical failures or resource shortages. ■ Develop and promote resources to improve the implementation of contingency plans.