Institute *for* Responsive Government

BRIDGING DIVIDES

Recultivating Election Security and Trust

BY KATHY BOOCKVAR & MATT CRANE

DECEMBER 10, 2025

Every day brings shocking reminders how inflamed distrust and division, paired with attacks on our electoral process, pose a growing threat to our national security. Recent acts of political violence against Democratic Minnesota House Speaker Emerita Melissa Hortman and her husband, as well as conservative activist Charlie Kirk, underscore that no ideology is immune. And as recently as the 2025 general election, hundreds of election officials, judges, and other public servants also faced threats, intimidation, and harassment, simply for doing their jobs. This is unconscionable, untenable, and painfully un-American.

As former election officials from opposite sides of the aisle, we've had the privilege — and the challenge — of supporting and administering elections for decades, during some of the most tumultuous years in modern American history. Still, neither of us could have predicted the pace or magnitude of the challenges that have emerged over the past five years — polarization accelerating into hostility; false narratives and propaganda sharpening every divide; and escalating attacks on the very bedrock of our electoral system.

The most striking shift has been that distrust and divide are no longer principally a tool by foreign adversaries as was the case for many eras; they are now also being stoked by homegrown and relentless domestic operatives. The consequences are grim: Thirty percent of U.S. adults now believe that political violence might be necessary to "get the country back on track," according to a 2025 NPR/PBS poll. That belief is not merely alarming; it is a threat to our nation itself — a constitutional republic that has stood for nearly 250 years.

The doubts that hang over U.S. elections did not appear overnight — they were planted, cultivated, and spread over decades, watered by both foreign adversaries and domestic opportunists. Over the last five years, those seeds have been supercharged by the nonstop flow of information and disinformation that reaches nearly every American through a phone screen. Making matters worse, the second Trump administration has made sweeping cuts to cybersecurity, intelligence-sharing, and other federal support, undermining nearly a decade of progress, while also appointing to key federal positions individuals who have widely propagated false conspiracy narratives.

Yet, across states and communities, we continue to see the seeds of resilience — local collaboration, bipartisan partnerships, and American voters who still believe, at their core, in fair elections. To recultivate security and trust, this moment requires clarity about how we got here and the conviction to move forward.

Kathy Boockvar (D) and Matt Crane (R) have worked for decades at the local, state, and federal levels to support and strengthen election security and administration. Crane previously served as Arapahoe County, CO Clerk and Recorder; as consultant to the Cybersecurity and Infrastructure Security Agency's Election Security Initiative; and is currently the Executive Director of the Colorado County Clerks Association, where he supports 64 clerks across the state. Boockvar previously served as the Pennsylvania Secretary of State and chief election official; as Vice President of Election Operations at the Center for Internet Security overseeing the EI-ISAC; and as a poll worker; and is currently President of Athena Strategies, an election security consulting firm.

Matt Crane

Matt Crane is an election subject matter expert committed to using his 25 years of election administration experience to assist the election community with improving operational and security processes to help build trust and confidence in American elections.

Matt currently serves as the Executive Director of the Colorado County Clerks Association, a not for profit 501 c (6) professional association that comprises 63 elected county clerk and recorders. Matt also served as an election official in Colorado for 19 years at both the state and county level.

Kathy Boockvar

Kathy Boockvar is President of Athena Strategies LLC, working to fortify election security, strengthen democracy, and amplify understanding and civil discourse about elections in the United States. Formerly Vice President of Election Operations for the Center for Internet Security (CIS), Kathy led its election security initiatives, working closely with federal, state, and local government to provide the highest standards of election security and cybersecurity practices and systems.

Ms. Boockvar previously served as Pennsylvania Secretary of State and chief election official, leading the Department of State to implement secure and resilient elections, protect the health and safety of the public through professional licensure, and support economic development.

1. FROM FOREIGN INTERFERENCE TO HOMEGROWN DISTRUST

A Shortened History of a Long-Brewing Vulnerability

Foreign efforts to influence U.S. elections and public opinion stretch back to before the Cold War, but the 2016 election marked a watershed in the modern cyber era — it was the first known large-scale attempt by a foreign adversary to target the machinery of America's election system itself. Russia's efforts to probe state systems, target vendors, breach party networks, and flood social media with disinformation showed that our adversaries understood a fundamental truth: If you can fracture trust in elections, you can fracture a nation.

The interference did not change election results, thanks to decentralized systems and vigilant government officials. But the public conversation quickly shifted away from the attacks themselves and toward political combat over alleged collusion. The result was that the real lesson — that the United States had entered a new era of asymmetric information warfare — never fully reached the American public. Thankfully, professionals and officials in the security sector understood immediately that this was a wake-up call. In the final days of the Obama administration, the Department of Homeland Security (DHS) designated election systems as *critical infrastructure*, providing stronger federal support so that state and local officials didn't have to face cyberwarfare alone.

The first Trump administration became an active partner to election officials nationwide. They established the Cybersecurity and Infrastructure Security Agency (CISA) and offered security tools, vulnerability scans, penetration testing, and cybersecurity training to state and local officials. Between 2017 and 2020, states and the federal government bolstered security together; FBI intelligence sharing, National Guard cyber teams, and coordinated federal agency task forces all helped strengthen defenses. State and local jurisdictions ran tabletop exercises, hardened networks, strengthened training and contingency plans, and built multi-agency partnerships. National Information Sharing and Analysis Centers (ISACs) provided intelligence and cyber support to offices in every region. Through these partnerships, from 2017-2024 CISA and other federal agencies ultimately provided election security support to more than 6,000 state and local election offices across the country.

The results were tangible. During the 2018 general election, security and election officials across the country were connected in real time through virtual situation rooms, sharing intelligence faster and more broadly than ever before. The partnerships weren't perfect, funding gaps persisted and smaller jurisdictions still lacked resources, but the line held. Over the next two years, the collaboration deepened, which became even more critical when 2020 arrived.

The 2020 stakes were magnified by three converging crises. First, the pandemic: Hundreds of thousands of American casualties, businesses shuttered, jobs lost — all while election officials were preparing for a major presidential election. Second, social media had become a nonstop global amplifier, where false information could spread instantly without accountability. Third, some political leaders, including the president and his allies, began broadcasting false claims, leveraging that same information superhighway to inflame distrust.

When that perfect storm hit, the partnerships built over prior years helped election officials adapt in real time, preserving both safety and access. What they achieved was extraordinary: Unprecedented transparency, more safe voting options for voters and election workers alike, secure operations, and the highest turnout in U.S. history. The defensive structure held firm. Cyberattacks were detected and mitigated, threat intelligence was shared swiftly, and when the votes were counted, experts agreed, the 2020 election was the most secure in U.S. history.

Those who understand election administration recognized it as an unparalleled triumph. Yet, the stronger the defenses became, the louder the conspiracy machine grew. Foreign interference had planted the seeds, but domestic voices cultivated them, becoming the mouthpiece for the same foreign actors intent on undermining our democracy. The reality that thousands of state and local election officials successfully protected the electoral system was buried under waves of conspiracy theories, disinformation, and political spin.

The achievement of a coordinated federal-state-local partnership — leveraging the full weight of America's intelligence and defense communities — should have been celebrated as a bipartisan success. Instead, it was drowned out by narratives of fraud and manipulation. By the end of 2020, the conversation had shifted from how much stronger the system had become to whether it could be trusted at all. Seeds of doubt, planted by foreign adversaries, had begun to take root.

Domestic Voices Take Over the Disinformation Playbook[2]

By 2020 and the years that followed, foreign disinformation operations increasingly blurred with domestic efforts. American influencers, partisan actors, and political operatives discovered the potency of sowing distrust. Long-standing, secure processes like vote-by-mail became targets for disinformation. Delays caused by record turnout, unprecedented mail volume, and the laws in a few states that prohibited mail ballot processing before Election Day, were portrayed as evidence of manipulation. Courts rejected case after case of fraud claims, and audit after audit confirmed the results were accurate, but the damage was done. What began as foreign interference matured into a self-sustaining domestic industry provoking distrust and divide.

Election officials, historically behind-the-scenes public servants, were suddenly vilified far and wide. Online harassment escalated into threats, intimidation, and doxxing. The line between domestic extremists and foreign agitators blurred: Armed American groups called for protests outside the homes of secretaries of state; Iranian operatives created a fake American-looking website, *Enemies of the People*, targeting election officials with their faces in sniper's crosshairs. The result? Experienced election administrators left the field in unprecedented numbers. A 25-year study by UCLA and the Bipartisan Policy Center found that average turnover among election officials rose from 28% in 2004 to 39% by 2022, and reached its highest point to date – a 41% turnover rate – in 2024. The reasons and dynamics vary from jurisdiction to jurisdiction, but contributing factors commonly cited include increasing threats, harassment, political pressure, and inadequate resources.

Between 2022 and 2024, the scope of threats grew dramatically. Federal and state law enforcement received thousands of reports. Threats expanded to mailed white powder, bomb threats, swatting, doxing, and incendiary devices on ballot drop boxes. In response, federal partners expanded critical support. CISA conducted thousands of physical security and cybersecurity assessments, trainings, and tabletop exercises. We witnessed firsthand the strength of the real-time intelligence-sharing, cyber defense, and incident response shared by the FBI, the ISACs, and state National Guard units. These efforts mattered. They helped detect attempted breaches, counter disinformation about the time, manner and place of elections, and prepare officials for crisis response.

But by 2024, distrust had become its own political currency. Candidates campaigned not only against opponents but also against the election system itself. Rejecting results became a fundraising tool and a partisan litmus test. What foreign adversaries once worked to import had become fully homegrown.

[2] *For more information on domestic misinformation during the 2020 election, please see Stanford University's Election Integrity Partnership report.*

2. WHERE WE STAND NOW: THE CONSEQUENCES OF FEDERAL RETREAT

The resilience built between 2017 and 2024 did not happen by accident — it was the product of bipartisan resolve, sustained federal investment, and thousands of election officials who adapted under extraordinary pressure. That progress, however, has now been eroded. Much of the election security support and services launched successfully by the first Trump administration have been dismantled by the second — the most significant setback in nearly a decade: CISA's Election Security and Resilience team has been dissolved; funding for the ISACs first reduced and now slashed; DHS's Foreign Influence Task Force was disbanded; the DOJ Election Threats Task Force shuttered; CISA's Regional Election Security Advisors who served as trusted liaisons to local officials are gone; and most field-based CISA services have been significantly curtailed. While the formal "critical infrastructure" designation remains in name, the ecosystem that made it meaningful has been hollowed out.

These cutbacks arrive at the same time that foreign and domestic adversaries are deploying more sophisticated tools, including AI-driven disinformation and social-engineering operations. They arrive as domestic influencers continue to amplify conspiracy theories about equipment, procedures, and election staff. And they arrive as state and local election offices face historic turnover, increased threats, and expanding responsibilities. Meanwhile, false information about vote-by-mail and voting-system technology — debunked repeatedly in courtrooms, audits, and bipartisan reviews — has resurfaced with new intensity, amplified by figures now positioned inside the federal agencies meant to protect election infrastructure.

State and local election officials, on the front lines of democracy, have felt the consequences already, followed by the voters they serve. The impact is significant: Officials are losing the very tools and services that helped them anticipate threats, harden their systems, and respond quickly when attacks occurred; while concurrently receiving far fewer federal dollars. This is a double hit, leaving local jurisdictions more exposed and forced to shoulder costs and risks they were never equipped to absorb. According to a 2025 Brennan Center survey, 60% of local officials are concerned about the loss of federal services; 87% said they now need greater support from state or local governments; 59% worry about political interference; 81% fear the accelerating spread of false information; and almost 40% have faced threats or abuse personally. The firebombing of the Archuleta County, Colorado election office in June 2025 is one of many attacks that underscores how real - and urgent – these needs have become.

These numbers are not abstract — they reflect a workforce and ecosystem being forced to absorb immense strain with far fewer tools. They represent real people — clerks, registrars, county directors – who live in the communities they serve and who continue showing up, driven by their exceptional commitment. And while the nation's defenses have been weakened, the resilience built over the last decade offers a foundation to rebuild. The bipartisan resolve that built the post-2016 security framework can take root again if the country chooses to invest in it, with the same clarity and urgency that made it strong the first time.

3. RECULTIVATING ELECTION SECURITY STRENGTH AND TRUST

Even without consistent federal partnership, states and localities are not starting from scratch. The last decade created a blueprint for what works — strategic investment in people and systems, collaboration across agencies, and clear communication with the public. These efforts cannot fully replace the loss of federal resources, but they can significantly strengthen resilience and restore confidence where voters interact most directly with their democracy.

The challenges ahead are not only technical, but also cultural. Hardening networks matters; so does hardening norms. The antidote to a years-long campaign of doubt is not a single message or widget — it is millions of trusted interactions that make the election process visible, verifiable, and human again. Republicans and Democrats alike, as well as nonprofit, academic, and private sector partners, must reinforce the security and integrity of our elections — no matter who wins.

Strategic Investment in Election Infrastructure

Election infrastructure cannot be maintained on good will alone. Federal Help America Vote Act (HAVA) grants once provided hundreds of millions of dollars in critical funding, but appropriations have steadily declined even as security demands have grown. To ensure stability, Congress should renew substantial, predictable funding that allows states and counties to keep pace with evolving security needs. States and local governments should also explore other funding avenues including:

- Dedicate state and local appropriations, bond funding, and/or grant programs to election security as Colorado recently did when the state passed legislation to reimburse all counties forty-five percent of all election related expenses for each election;
- Use allowable portions of cybersecurity or emergency-management funds to strengthen election networks.
- Incentivize public-private partnerships for technology innovation, training, and physical-security upgrades;
- Explore creative approaches to election funding, such as utilizing unclaimed funds; checkoff initiatives; or leveraging state or federal infrastructure funds; and
- Explore programs helping to provide affordable pooled services and information-sharing.

Embedding election funding into regular budgets, not sporadic emergency allocations, will dramatically strengthen long-term resilience. Secure, reliable elections are as essential to public infrastructure as roads, water systems, and emergency response.

Cross-Sector Collaboration and Resource-Sharing

One of the most effective ways to fill federal gaps, strengthen security, and expand information and resource-sharing is through sustained collaboration among election officials, emergency management, law enforcement, cybersecurity teams, and communications professionals. States with mature inter-agency and/or cross-state partnerships, such as Pennsylvania, Montana, Washington, and North Dakota, have shown how a practice of routine coordination can break down silos and accelerate election security and preparedness. Strong state election official associations, such as the Colorado County Clerks Association, also play a critical role by facilitating collaboration, sharing best practices, and ensuring that timely information reaches even the smallest and most remote jurisdictions. These partnerships are not formulaic; each jurisdiction can tailor its model based on available expertise and operational needs.

Collaboration between election personnel and law enforcement has been particularly constructive. The Committee for Safe and Secure Elections (CSSE), a bipartisan network of election and law enforcement professionals, helps jurisdictions by providing resources, training, and tabletop exercises to help officials protect voters and workers. Georgia has taken this a step further by pioneering a requirement for election-security training for all new police officers. Every state should consider similar mandates so that law enforcement understands both the legal framework and nuances of protecting election infrastructure. Cross-agency partners can also lend their expertise by helping to perform physical security assessments of election facilities, and district attorneys and other law enforcement partners should ensure that laws against threats or obstruction are enforced.

Cyber navigator programs offer another cost-efficient model. By dedicating state cybersecurity specialists to assist local election offices, states have been able to identify vulnerabilities, test systems, and coordinate incident response more effectively. These roles have helped engender faster mitigation, stronger communication pathways, and improved confidence among local officials.

Spreading the Word about our Elections

And as we've seen, even the strongest cyber defenses cannot withstand an unchecked flood of false narratives. Americans are awash in misinformation and conspiracy theories. Because no single message or entity can counter disinformation at this scale, progress depends on millions of individual conversations — between neighbors, in schools, at community centers, and online.

Both of us have seen how powerful these conversations can be. Kathy has been driven by a powerful conversation with a woman on a plane, yearning to understand more about the 2020 election. After learning how votes are cast securely and election results observed and verified, the woman expressed her fervent wish to share this information with her community – if only she had "the right words." Matt has had similar experiences — people who initially were skeptical of the 2020 election results later told him how valuable their conversations had been in helping them explain to others that the election wasn't stolen. Many of them still call Matt with new questions, wanting to make sure they get the facts right before passing information along.

These exchanges remind us that trust grows through proximity. When people understand how elections work and why adversaries sow doubt, they become advocates in their own circles. Helping Americans find those words and trust is one of the most powerful antidotes to disinformation. Transparency and encouraging skeptics to become part of the process – especially as poll-workers – can be immensely constructive. Equally important is amplifying trusted voices and fostering a society-wide knowledge base and commitment to sharing accurate information that meets people where they are.

One of the most important parts of "the right words" is to help people understand the heroes of our democracy — the individuals who administer our elections. Our elections are run at the local level by our neighbors. They are not part of some political conspiracy; to the contrary, they are civil servants, bound by law, guided by bipartisan oversight, and committed to accuracy and transparency. They are the unseen stewards of democracy, often working 12- to 16-hour days for weeks before and after Election Day, testing equipment, mailing ballots, staffing polling places, verifying results, and conducting audits. They don't take sides; they follow the law. Their dedication deserves both gratitude and protection.

Every attack on our electoral process and every act of political violence heightens the threat to our national security and to every citizen's ability to vote freely. Ultimately, sustaining a healthy democracy depends on millions of everyday exchanges — in living rooms, classrooms, workplaces, and digital spaces — where Americans help one another separate fact from fiction, build trust, and stand with those who safeguard our elections.

CONCLUSION
Country Over Party, Fact Over Fear

As the nation marks 250 years since the Declaration of Independence, we face a choice. We can allow distrust and division to define our democracy. Or, we can recommit to the simple, radical promise that has carried us this far: American citizens choose their leaders in free, fair, and secure elections and accept the vote of the populace when the counting is done, whether “our” candidate won or lost.

This will require honest investment, practical cooperation, and civic courage. It will require Republicans, Democrats, and independents alike to elevate country over party, and fact over fear. The good news is that the blueprint already exists — state and local election officials model it every day. At the end of the day, we have built these defenses before. We know collaboration works and we know transparency and understanding build confidence. The work ahead is not easy, but it is clear and it is ours. If we choose it together, we can recultivate election security and trust and hand a stronger democracy to the next generation.