

**Committee on Homeland Security  
United States House of Representatives  
Democratic Forum**

**“Defending Democracy: Protecting Elections from Executive Overreach”**

**Written Statement of Lawrence D. Norden  
Vice President, Elections and Government Program,  
Brennan Center for Justice at NYU School of Law**

**April 28, 2026**

Ranking Member Thompson and members of the Committee, thank you for the opportunity to speak about the impact of federal cuts to election security. As Vice President of the Elections and Government Program at the Brennan Center — an independent, nonpartisan law institute — I have been deeply involved in the effort to ensure election officials have the support they need to administer safe and secure elections.

The cutbacks to election security support from the federal government that began in early 2025 represent a serious and ongoing threat to the infrastructure that state and local election officials depend on to run safe and secure elections.<sup>1</sup> Since taking office, the Trump administration has cut security resources and services for states, pushed out the expert staff who previously ran these programs, and dismantled entities that monitored threats of foreign interference in elections. The administration also cut funding for the Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC), a nationwide network that facilitated information sharing about security risks and best practices between election vendors and election officials across state lines. The Brennan Center’s annual surveys of local election officials shows that they recognize the danger: 60 percent reported being concerned about federal cuts to election security services in 2025.<sup>2</sup> A year later, the gap has not closed. In our most recent survey, released this month, seventy-five percent said their state or local governments have not provided additional resources to address these cuts.<sup>3</sup>

There is, however, reason for measured confidence. Under our constitutional system, states run elections, and the decentralized structure of American election administration is itself a form of resilience. Over the past decade, election security has grown stronger — through near-universal adoption of paper ballots, hardened networks, and a deepened civil society ecosystem that can

---

<sup>1</sup> Lawrence Norden, “How the Federal Government Is Undermining Election Security,” Brennan Center for Justice, April 14, 2025, <https://www.brennancenter.org/our-work/research-reports/how-federal-government-undermining-election-security>.

<sup>2</sup> Brennan Center for Justice, *Local Elections Survey — July 2025*, July 10, 2025, <https://www.brennancenter.org/our-work/research-reports/local-election-officials-survey-july-2025>.

<sup>3</sup> Brennan Center for Justice, *Local Election Officials — July 2026*, April 13, 2026, <https://www.brennancenter.org/our-work/research-reports/local-election-officials-survey-2026>.

help absorb some of the shock of federal withdrawal. Most importantly, the people who administer our elections — across all fifty states, across both parties, in jurisdictions large and small — are professionals who serve because they believe in elections and democracy. The processes they oversee are bipartisan by design, transparent at critical junctures, and built with multiple layers of redundancy and verification. That foundation has not changed.

Importantly, there is still time before the midterms for states to deepen coordination within and across their borders, and that work has already begun in promising ways.

## **I. What Was Built — and What Has Been Dismantled**

The foundation for much of federal government's role in election security was built largely during the first Trump administration and expanded through subsequent years. In 2017, the Department of Homeland Security (DHS) designated election infrastructure as critical infrastructure following attempts by Russian actors to scan and infiltrate state election systems.<sup>4</sup> This designation provided states and localities with access to many of the cybersecurity protections that DHS offers other private and public entities, such as ongoing threat monitoring, risk and vulnerability assessments, and incident response support. In 2018, Congress created the Cybersecurity and Infrastructure Security Agency (CISA) as the entity within DHS that would be primarily responsible for carrying out critical infrastructure support — and therefore, election security support.<sup>5</sup>

Ahead of each federal election through 2024, CISA provided election offices nationwide with vital cybersecurity services to keep elections safe and secure, such as threat intelligence briefings, cybersecurity assessments, incident response support, vulnerability scanning, risk management training, and best practices on emerging security threats, all on a voluntary basis. In 2023 and 2024 alone, CISA conducted over 700 cybersecurity assessments and over 1,300 physical security assessments for local election jurisdictions around the country.<sup>6</sup>

The EI-ISAC, which CISA funded, was also important, and also created during the first Trump Administration. Because election administration is decentralized, with local officials across thousands of jurisdictions doing the day-to-day work, there was little visibility into what was happening beyond state lines for too long. But threats to elections rarely impact one county or even one state. They have implications for every election official, and those who seek to undermine American elections do not confine their attacks to one locality. The EI-ISAC, a nationwide information sharing and support network for election officials, was designed to address this problem. Its monitoring services not only protected individual election systems but gave all network participants visibility into patterns of activity across the country.

And it was not just CISA providing support. The Department of Justice, for example, set up an Election Threats Task Force following a rapid increase in threats, harassment, and abuse directed

---

<sup>4</sup> Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector (January 6, 2017), <https://www.dhs.gov/archive/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical>.

<sup>5</sup> Cybersecurity and Infrastructure Security Agency Act of 2018, H.R.3359, 115th Congress (2018), <https://www.congress.gov/bill/115th-congress/house-bill/3359>.

<sup>6</sup> Cybersecurity and Infrastructure Security Agency 2024 Year in Review (2024), <https://www.cisa.gov/about/2024YIR>.

at election officials, which had cause many to leave the field in fear for their safety.<sup>7</sup> The Task Force brought over 20 prosecutions against those who threatened election workers, and the FBI investigated threats that appeared to originate from abroad, including the more than 200 bomb threats targeting polling places on and after Election Day 2024.<sup>8</sup>

This entire apparatus has been substantially dismantled. CISA has greatly cut or deprioritized services for election officials, and the experts who managed this work in 2024 were terminated or put on leave.<sup>9</sup> DHS defunded the EI-ISAC, along with the companion Multi-State Information Sharing and Analysis Center (MS-ISAC), which served as the primary cybersecurity information sharing network for all government entities.<sup>10</sup> The Department of Justice disbanded the FBI's Foreign Influence Threats Task Force and Director of National Intelligence Tulsi Gabbard dissolved the Foreign Malign Influence Center, leaving election officials with less insight into how foreign adversaries may seek to undermine election security.<sup>11</sup> And through pardons of those involved in the January 6 attack on the Capitol, political interference, and consistent false claims of fraud and rigged elections, the White House has created an environment where more individuals may feel emboldened to threaten election workers and infrastructure without fear of consequences.<sup>12</sup> Taken together, the role that the federal government recently occupied as a central hub for election security support and coordination has been vacated.

Perhaps most damaging of all has been the erosion of trust. Some officials have indicated that regardless of what services the federal government might offer in the future, the disruption has compromised the relationship beyond easy repair. For example, in June 2025, hackers targeted the Arizona's Secretary of State's Office, gaining access to their online portal for political candidates and replacing candidate photos with images of the late Iranian Ayatollah Ruhollah Khomeini.<sup>13</sup> While Secretary of State Adrian Fontes immediately began working with state

---

<sup>7</sup> U.S. Department of Justice, "Guidance Regarding Threats Against Election Workers," June 25, 2021, <https://www.justice.gov/archives/dag/file/1160226-0/dl?inline>.

<sup>8</sup> U.S. Department of Justice, "Election Threats," updated May 5, 2025, <https://www.justice.gov/archives/voting/election-threats#ettf>.

<sup>9</sup> Adam Sella, "Trump's Gutting of Election Security Fuels Worries for Midterms," *New York Times*, March 17, 2026, <https://www.nytimes.com/2026/03/17/us/politics/trump-cisa-election-security.html>.

<sup>10</sup> Jule Pattison-Gordon, "The Feds Cut Funding for Election Cybersecurity. How Will Public Officials Adapt?," *Governing*, December 2, 2025, <https://www.governing.com/management-and-administration/the-feds-cut-funding-for-election-cybersecurity-how-will-public-officials-adapt/>.

<sup>11</sup> Steven Lee Myers, Julian E. Barnes, Sheera Frenkel, "Trump Dismantles Government Fight Against Foreign Influence Operations," *New York Times*, February, 20, 2025, <https://www.nytimes.com/2025/02/20/business/trump-foreign-influence-election-interference.html>; David Salvo, "What Just Happened? Dismantling the Intelligence Community's Foreign Malign Influence Center," *Just Security*, August 28, 2025," <https://www.justsecurity.org/119653/wjh-dismantling-foreign-malign-influence-center/>.

<sup>12</sup> President Trump has continued to falsely claim, among other things, that noncitizens are voting in large numbers, that mail voting leads to fraud, and that voting machines are rigged. And the administration has used these claims to justify unconstitutional executive action that would upend states' election procedures, to seek access to sensitive voter data and election materials, and to launch investigations against individuals who stood up for the accuracy of elections. Brennan Center for Justice, *Timeline of the Trump Administration's Efforts to Undermine Elections*, last updated February 9, 2026, <https://www.brennancenter.org/our-work/research-reports/timeline-trump-administrations-efforts-undermine-elections>. Similar false claims in the past have motivated individuals to threaten election workers, seek illegal access to voting systems, intimidate voters, and disrupt election processes. Derek Tisler and Lawrence Norden, *Securing the 2024 Election*, Brennan Center for Justice, April 27, 2023, <https://www.brennancenter.org/our-work/policy-solutions/securing-2024-election>.

<sup>13</sup> Jen Fifield, "Hackers who breached Arizona election website aimed at other targets, too," *AZ Mirror*, July 23, 2025, <https://azmirror.com/2025/07/23/hackers-who-breached-arizona-election-website-aimed-at-other-targets-too/>.

officials to investigate the breach, he delayed notifying CISA. Fontes’s reason was clear: his office had “lost confidence in [CISA’s] capacity to collaborate in good faith.” Of their current relationship with CISA, he said, “we have no [federal] cybersecurity advisors.”<sup>14</sup> That loss of confidence and coordination — a significant factor in America’s strengthened election security position since 2016 — is not something that can be easily replaced.

## II. Where Things Stand Now

State and local officials have not been passive in the face of these cuts. They are instead turning to state and local partners who may have the resources, expertise, and capacity to help fill the gap. Eighty-nine percent of officials plan to coordinate with at least one other local or state agency or department to prepare for a safe and secure election in 2026, with 80 percent planning to coordinate with law enforcement. Fifty-four percent plan to coordinate with state or local information technology (IT) agencies.<sup>15</sup> Around the country, State and local agencies are adopting a whole-of-government approach to securing elections, coordinating closely with election officials to ensure they are prepared for any challenge that arises.

Civil society is also playing a vital role. The Committee for Safe and Secure Elections (CSSE) — a collaboration between election administration and law enforcement leaders that formed to improve election safety after 2020 — has been providing trainings for election workers and law enforcement offices across the country while building relationships and strengthening coordinated response plans in the process.<sup>16</sup> Many of the election security experts that previously worked for CISA helped launch the Election Security Exchange, which provides threat analysis and security best practices for election officials through clear language and concrete takeaways.<sup>17</sup> The MS-ISAC continues to offer election security support to government entities, and at least 13 states have now bought into statewide memberships that offer election officials access to these services, with a number of other states, local jurisdictions and vendors gaining access through other arrangements.<sup>18</sup>

Yet the same officials who are preparing also know the gap caused by federal cuts endures. Only six percent say the state and local response has fully made up for what was lost.<sup>19</sup> It is also true that there are capabilities of the federal government — particularly in foreign threat intelligence and cross-jurisdictional information sharing — that no state or civil society actor can replicate on their own. The advances in Artificial Intelligence, and the threat that poses to cybersecurity and the information environment makes this pullback even more unsettling.<sup>20</sup>

---

<sup>14</sup> Derek B. Johnson, “After website hack, Arizona election officials unload on Trump’s CISA,” *CyberScoop*, July 21, 2025, <https://cyberscoop.com/arizona-secretary-of-state-website-hack-candidate-portal-criticizes-cisa/>.

<sup>15</sup> Brennan Center for Justice, *Local Election Officials — July 2026*, 3.

<sup>16</sup> Committee for Safe and Secure Elections, “Homepage,” accessed April 23, 2026, <https://safeelections.org/>.

<sup>17</sup> Election Security Exchange, “Homepage,” accessed April 23, 2026, <https://securingelections.org/>.

<sup>18</sup> Rae D. DeShong, “Vermont Becomes 13th State to Purchase MS-ISAC Membership,” *Government and Technology*, April 10, 2026, <https://www.govtech.com/security/vermont-becomes-13th-state-to-purchase-ms-isac-membership>.

<sup>19</sup> Brennan Center for Justice, *Local Election Officials — July 2026*, 5.

<sup>20</sup> Derek Tisler, “Election Officials Have Been Preparing for AI Cyberattacks,” Brennan Center for Justice, April 23, 2026, <https://www.brennancenter.org/our-work/analysis-opinion/election-officials-have-been-preparing-ai-cyberattacks>; Isabel Linzer and Tim Harper, “Countdown to the Midterms: The Changing AI Threat Landscape for Elections,” Center for Democracy & Technology, November 18, 2025, <https://cdt.org/insights/countdown-to-the-midterms-the-changing-ai-threat-landscape-for-elections/>.

### III. What Can Be Done

There is still time to act, and a clear agenda has emerged from conversations the Brennan Center has had with election security stakeholders across the country.

States should lean into the whole-of-government models that are already producing results,<sup>21</sup> for example by establishing inter-agency election working groups to identify and coordinate state support, tapping into existing expertise and capacity at state agencies to conduct trainings and risk assessments, and facilitating collaborative responses at the local level through scenario planning exercises.<sup>22</sup> Lawmakers can set baseline security requirements and provide election officials with sufficient funding to run secure elections.<sup>23</sup> Law enforcement leaders can collaborate with election officials on incident response, deter attacks on elections, and hold perpetrators accountable.<sup>24</sup> Election and security officials can establish and join interstate information-sharing networks to prepare for developing threats.<sup>25</sup> And all public leaders can clearly express that attacks on the workers and systems that run our elections will not be tolerated.

State legislators can also pass laws to protect voters and election infrastructure from federal interference. For example, they can create state crimes covering activity that is already illegal under federal law — such as deploying armed law enforcement to polling places or interfering in an election — to ensure that federal officials who violate these laws can be held prosecuted under state law as well.<sup>26</sup> Federal officials are immune from state criminal prosecution only if

---

<sup>21</sup> Derek Tisler and Chris McIsaac, *A State Agenda for Election Security and Resiliency*, Brennan Center for Justice and R Street Institute, July 24, 2025, <https://www.brennancenter.org/our-work/policy-solutions/state-agenda-election-security-and-resiliency>.

<sup>22</sup> States such as Montana, New Jersey, and Pennsylvania have state inter-agency working groups to identify available election security support and ensure alignment in delivery. Georgia utilizes its state emergency management agency to conduct cybersecurity scans and assessments for election officials. Election officials in Florida and Michigan partner with universities, non-profit organizations, and other experts to host tabletop exercises on election security. *Id.*

<sup>23</sup> Brennan Center for Justice and State Futures, *How State Legislators Can Protect Election Integrity and Security*, January 5, 2026, <https://www.brennancenter.org/our-work/research-reports/how-state-legislators-can-protect-election-integrity-and-security>.

<sup>24</sup> Committee for Safe and Secure Elections, *Five Steps to Safer Elections*, accessed April 24, 2026, <https://safeelections.org/five-steps-to-protect-our-elections-from-the-committee-for-safe-and-secure-elections/>.

<sup>25</sup> At least ten states have joined the Joint Cybersecurity Operations Command Center, which allows state IT and cyber officials to directly share threat intelligence without a national intermediary. Benjamin Freed, “North Dakota’s Interstate Cyber Operations Center Expands to 10 States,” *Statescoop*, August 18, 2022, <https://statescoop.com/north-dakota-interstate-cyber-operations-center-expands-10-states/>. At least 13 states have bought into MS-ISAC’s State & Territory-Wide Membership, which extends access to cybersecurity services and information sharing to all government entities within the state, and includes a Threat Intelligence Package for Elections. Center for Internet Security, *MS-ISAC State & Territory-Wide Membership*, <https://learn.cisecurity.org/MS-ISAC-State-and-Territory-Wide-Membership-Model>; Center for Internet Security, *MS-ISAC Threat Intelligence Package for Elections*, [learn.cisecurity.org/MS-ISAC-Election-Threat-Intelligence-Package](https://learn.cisecurity.org/MS-ISAC-Election-Threat-Intelligence-Package). Even without any additional funding or state approval, election officials can access security best practices and subscribe to receive updates on emerging threats through the Election Security Exchange. Election Security Exchange, <https://securingelections.org/>.

<sup>26</sup> Patrick Berry and Derek Tisler, “Model Bill: State Accountability for Federal Interference at Polling Places,” Brennan Center for Justice, April 15, 2026, <https://www.brennancenter.org/our-work/policy-solutions/model-bill-state-accountability-federal-interference-polling-places>. New Mexico passed a similar bill earlier this year. New Mexico S.B. 264 (2026), <https://www.nmlegis.gov/Sessions/26%20Regular/final/SB0264.pdf>.

they are engaged in conduct that is authorized by federal law and the official's actions were "necessary and proper" in fulfilling their federal duties; they can therefore be subject to state prosecution for actions that are clearly illegal under federal law.<sup>27</sup> State legislators can also pass laws to strengthen the chain of custody of voting equipment, ballots, and other election materials, and restrict these materials from being turned over to a third party absent a court order.<sup>28</sup>

Finally, all Americans must be aware that foreign adversaries and even our own federal government may try to undermine faith in elections. The non-stop flood of false claims about election integrity since 2020 continues to do immense damage to election administration even though these claims have been thoroughly and repeatedly debunked. This year, 74 percent of election officials said they are concerned about the spread of false information making it more difficult or dangerous to do their job (against a backdrop where one in three of those officials had already faced threats, harassment, or abuse for doing their jobs).<sup>29</sup> As the Trump administration seeks to seize election materials, private voter registration data, and relitigate the 2020 election, the President and other leading officials have continued to spread rumors and false information about our elections, but this time with the seal of the federal government.<sup>30</sup>

Leaders across government, business, civil society, and within communities must stand by the professional work of election officials, understand the protections that keep elections safe and secure, and use their platforms to support those protecting the integrity of our system, while encouraging trust and participation in the democratic process. The networks that previously existed to support election integrity and to push back on false claims have diminished. We all have a role to play rebuilding that connective tissue and preparing Americans for any challenges to free and fair elections this year.

The good news is that the system itself is resilient. Nearly every vote now has a paper record that can be reviewed and audited, meaning that we have the ability to verify the accuracy of vote counts across the country. States run elections and count ballots using bipartisan processes that

---

<sup>27</sup> See Bryna Godar, *Can States Prosecute Federal Officials?*, State Democracy Research Initiative, July 17, 2025, <https://statedemocracy.law.wisc.edu/our-work/can-states-prosecute-federal-officials>.

<sup>28</sup> Some of the ways states have strengthened protections for voting systems and ballots include requiring election officials to maintain strict custody of voting machines (Maine, 21-A § 845), requiring a court order to open ballot containers (Washington, RCW 29A.60.110), making it a crime for individuals outside of election workers and voting system vendors to access voting systems (Colorado, CO Rev Stat § 1-13-708; California, Cal. Elec. Code § 18564), and requiring election officials to notify the state election office whenever an official receives a written or verbal request for third party access to voting systems (California, Cal. Elec. Code § 18564; Pennsylvania, Directive 1 of 2021). California is currently considering a bill that would prohibit election officials from permitting a federal government agency or its employees to inspect a voting system, unless authorized by court order. California S.B. 73 (2025), [https://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?bill\\_id=202520260SB73](https://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?bill_id=202520260SB73).

<sup>29</sup> Brennan Center for Justice, *Local Election Officials — July 2026*.

<sup>30</sup> Derek Tisler and Lawrence Norden, "Beware of Novel Claims of 2020 Election Fraud," Brennan Center for Justice, March 13, 2026, <https://www.brennancenter.org/our-work/research-reports/beware-novel-claims-2020-election-fraud>. As recently as April 22, President Trump was stating that the Virginia's Redistricting Referendum was "a rigged election" where "Republicans were winning . . . until . . . a massive 'Mail In Ballot Drop!'" Donald J. Trump (@realDonaldTrump), Truth Social, April 22, 2026, <https://truthsocial.com/@realDonaldTrump/posts/116449559745815736>. FBI Director Kash Patel recently promised on Fox News that arrests related to the 2020 elections will be coming soon, just days after DOJ sent a letter to election officials in Michigan demanding records related to the 2024 election. Jacob Wendler, "Trump DOJ Redoubling Election Scrutiny Efforts," Politico, April 19, 2026, <https://www.politico.com/news/2026/04/19/trump-doj-redoubling-election-scrutiny-efforts-00880159>.

are transparent and observable by the public. They develop and implement backup plans to ensure that voting can continue through disruption, and they layer in checks and balances to confirm accuracy and security every step of the way. And election officials remain committed to their work. They are planning for potential disruptions to the midterm elections and showing the same resilience they have repeatedly demonstrated in recent elections in the face of a pandemic, political interference, threats, and even violence.

Democracy ultimately depends on participation. Participation by voters. Participation by poll workers. Participation by leaders in law enforcement, cybersecurity, and emergency management, supporting election officials and keeping elections safe and secure. Participation by lawmakers protecting and strengthening election processes and giving election officials the resources needed to secure their systems and serve voters. Participation by attorneys general defending those systems against external threats and interference. And participation by all Americans, standing up for free and fair elections, supporting the work of election officials, and demanding that public officials abide by the will of the people.