



ACET to Washington: Many of the Election Security Fixes You're Demanding Are Already Standard Practice

ACET statement in response to recent election technology claims

WASHINGTON, D.C. (July 19, 2026) — The President's address, Secretary Mullins' remarks, and corresponding document release focused on threats to U.S. elections calling for stronger safeguards. The American Council for Election Technology (ACET), a national, nonpartisan trade association for election technology providers, does not dispute that the threats are real. But our response is simple: we're already doing the work.

Most of this week's release covers ground that's been assumed or publicly known, in some capacity, for years. The one new document, [the CISA Elections Report](#), publicizes that election technology providers have spent years working with federal researchers to find and fix vulnerabilities. Moreover, several of CISA's recommendations—which Secretary Mullins characterized as mitigation steps that can be taken today—describe practices ACET members already follow. Others recommendations identify regulatory and funding gaps only government can close. Of note, nothing in the CISA report shows a nation state altered a single vote or changed a result. “Unlike Venezuela, America has the receipts. We can show the security and accuracy of our elections through our system of built-in transparency and accountability. Just like how our voter-verifiable paper audit trail and every credible review shows no interference,” said ACET Executive Director Sara Cutter. “But our members don't need a smoking gun to take a threat seriously. They've spent years working to prevent a successful attack.”

The report's discussion of the Critical Product Evaluation (CPE) program provides the clearest example of the work ACET members have done. Between 2019 and 2024, voting system manufacturers voluntarily submitted equipment to Idaho National Laboratory so federal researchers could identify vulnerabilities. The purpose was to find weaknesses during research and development, fix them, and strengthen the system *before* deployment. Which is why ACET disagrees with the report's suggestion that this cooperation model resulted in a lack of disclosure. Finding vulnerabilities with the nation's top security researchers was the entire point of the exercise. But the testing

occurred during the research and development phase under laboratory conditions. Regulators do not typically require disclosure of every bug found and fixed while a product is still being built. “Election technology providers voluntarily invited government experts to look for problems before adversaries could,” Cutter said. “Treating voluntary, pre-market security testing as evidence of misconduct discourages collaboration.”

Beyond the CPE program, the report also lists six mitigation recommendations, which describe practices ACET members already follow or support. First, ACET members have pushed for years to align disclosure and certification timelines, but only regulators can build the security-only review track that would let patches move quickly.

“Washington is asking why security updates cannot move at normal cybersecurity speed while maintaining a regulatory structure that prevents exactly that,” Cutter said. “Define a security-only review track, preserve testing and change orders, and remove the procedural delay.”

Second, CISA's best practice checklist including access controls, network segmentation, multifactor authentication, monitoring, and logging is already built into ACET members' products and support services. Third, around 98% of votes cast in 2024 were recorded on paper, and approximately 79% of registered voters live in jurisdictions where the primary voting system tabulates human-readable marks or text rather than QR codes or barcodes. ACET members are already moving towards eliminating encoded votes as a ballot-marking device default or as a tabulation method. Fourth, as of April 30, every state runs a post-election audit. Fifth, providers already assign CVEs, notify customers of breaches, report incidents, and provide software bills of materials through the channels available to them (customers, state officials, VSTLs, and the EAC) even though no single federal channel exists to receive them. Sixth, documentation of incidents and remediation, at least internally, is likewise already standard for many providers. Making it a consistent and public everywhere is a policy call, not a provider one. “Election technology providers cannot report into a process that does not exist or changes from state to state,” Cutter said. “Create a clear channel, protect sensitive security information, define who receives it, and set consistent reporting standards. ACET members will participate.”

Voter registration and electronic pollbooks, though outside the report's focus on voting systems, already support most of these same protections. Moreover, these technologies are central to the administration's own priorities on proof of citizenship, voter ID, list maintenance, and interstate matching.

Finally, Secretary Mullin raised concerns about foreign-supplied components embedded in election systems. Foremost, ACET members share the goal of a secure supply chain. Moreover, ACET member companies do not source hardware components from North Korea, Russia, or Iran. Our members also recognize that geography alone cannot

establish whether a component is safe. “Assessing risk mainly by where a part was assembled creates false confidence,” Cutter said. “Our members are skeptical of components regardless of country of origin.” Providers already run NIST-based supplier risk assessments, conduct site visits, screen for counterfeit parts, trace firmware dependencies, and track chain of custody from manufacture through delivery and reserve the sharpest scrutiny for components that store data and execute code.

“Washington is demanding we start things we’ve achieved. And it’s asking for outcomes it has made harder to deliver. The EAC can’t set policy without commissioners. States can’t modernize without funding. Rules can’t be streamlined without someone to convene the work,” Cutter said. “Fund elections. Modernize the infrastructure. Keep the paper and the audits. Harmonize the rules. Verify the supply chain. We’re already doing our part. It’s time for Washington to do theirs.”

###

About ACET

The American Council for Election Technology (ACET) is a national, nonpartisan trade association founded in 2022. Our mission is to advance policies and programs that support the use of election technology to ensure secure, accurate, and transparent elections. ACET provides a collaborative platform for industry leaders to address challenges and develop solutions for election security and accessibility. Our members include major voting system manufacturers, election technology providers, and innovators in ADA compliance. Together, we are a unified voice advocating for policies that build public trust and advance security.

For more information, please visit TechForElections.VOTE or contact press@techforelections.vote.

Follow ACET on [LinkedIn](#) and [X](#) for updates.