Our government tested election security; it failed

Why are Americans only now finding out?

Washington Times, Page B1, By Peter Navarro, August 17,2026

Picture a break-in where the burglars are the good guys.

From 2019 through 2024, federal cybersecurity teams were invited to probe election software and networks. The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency conducted penetration tests and red-team operations against state and local networks, while CISA and the Idaho National Laboratory worked with election vendors to tear into election software.

Their mission was straightforward: Find the weak points before real adversaries could exploit them.

Newly released government documents — including a retrospective CISA report and declassified intelligence records — reveal both how vulnerable some election systems have been and how long the government has known about the threats.

The CISA report reveals that "in multiple cases, CISA assessors gained full network control within hours or days." Many state and local partners, it warned, "remain soft targets incapable of stopping even moderately skilled adversaries."

The break-ins were possible for a simple structural reason. Election systems that were supposed to be isolated often were not. Get into an ordinary government office network — the network carrying email and office applications — and in some cases, you could reach election systems.

Translation: The walls that everyone assumes separate election systems from ordinary office computers can be porous. CISA found election systems reachable from enterprise networks, with firewall gaps and supposedly "isolated" equipment quietly still connected.

Worse still, CISA says some election systems are "locked down" against changes for weeks or months before Election Day, and in some cases, those lockdown periods are mandated by state law.

Certification requirements can also delay security updates. CISA does not identify the states. But its warning is explicit: Some certification regimes “require that no patches be applied for months before an election.”

Read that again. In some jurisdictions, rules meant to protect election systems can prevent officials from fixing a known security hole during the very period an adversary has the greatest incentive to exploit it.

The result, according to CISA: “known, documented vulnerabilities persist for months or years” on production election systems.

Then there are the voting machines themselves, the third rail of election-denier politics — the Voldemort words that one dares not speak.

CISA’s new report revives a warning that has been sitting in plain sight for years. A 2021 expert report filed in federal court in Georgia found that ballot-marking devices encoded voters’ choices in bar codes which “voters had no way to verify.”

The researcher demonstrated that those encoded choices could be altered without physical access to the machines. To be precise, the analysis showed that votes could be changed (not that they actually were).

What is striking is that CISA is still citing the vulnerability in 2026 — and still recommending human-readable paper ballots.

And what about who controls the companies that build our voting systems? A newly released January 2020 National Intelligence Council memo proposed a simple safeguard called “Third-Party Vendor Verification” whereby companies that manufacture or transship election infrastructure would be screened for shared vulnerabilities and insider threats.

The concern was not theoretical. A separate CIA review released this summer, drawing on intelligence dating back to 2004, recounts how Smartmatic’s acquisition of U.S. voting-system company Sequoia triggered a 2006 intelligence community national-security assessment.

That assessment rated the acquisition a “moderate” threat to U.S. national-security interests, and the CIA review says subsequent Committee on Foreign Investment in the United States pressure resulted in Smartmatic divesting Sequoia in 2007. Let’s be clear — and clear-eyed. This is a bipartisan issue ripe for action on the Hill. America’s election infrastructure is a target for anyone who would seek to manipulate or disrupt our elections.

With fewer than 90 days before what may be one of the most consequential congressional elections in our history, Congress should act. The 2026 general election is Nov. 3. The government has already written the prescription, if not the bill. Stop certification rules from blocking security fixes.

If a vulnerability is found in October, election officials should be able to patch it that month — not wait until after the election. CISA itself recommends harmonizing patch-management and certification rules so cybersecurity changes can be made in real time without jeopardizing certification. Mandate human-readable paper ballots and manual audits of those ballots before results are certified.

Require vendors to do what CISA now recommends: Assign CVE numbers to vulnerabilities, notify customers if source code is leaked or stolen, report cybersecurity incidents, provide a software bill of materials and transparently document incidents and remediation.

Build the vendor-verification screen requested by the intelligence community in 2020 — and include foreign ownership and control in the review. We scrutinize the companies that build our weapons. We should also scrutinize the companies that build our voting systems.

The most troubling question may be why Americans are only now getting this consolidated picture. Much of the testing occurred years ago. CISA's own report says its election-software evaluation program with the Idaho National Laboratory ran from 2019 through 2024, and final reporting on that program concluded in 2025.

Now we have a public CISA report pulling the findings together, including the stunning admission that federal testers sometimes gained full network control within hours or days. Congress should find out why this consolidated public accounting came only now.

Peter Navarro is assistant to the president and senior counselor for trade and manufacturing.