“Not Connected to the Internet” – The Dangerous Deception That Has Misled a Nation

July 13, 2026

You have heard it repeated for years: our voting systems are secure because they are “not connected to the internet.” That single phrase has shaped how millions of Americans, election officials, and journalists think about election security. It has skillfully conditioned the public to believe that the only real threat is an internet connection. This belief is false; and dangerously misleading.

The internet is merely one network among millions. There are over 120,000 autonomous systems forming the global internet, and when private networks, local connections, cellular APNs (what most poll-books use), and proprietary wireless systems are included, the total reaches into the millions. Citizens have been trained to ask only one narrow question while ignoring the much broader attack surface.

A voting system does not need to touch the public internet to be manipulated. Wireless cards remain physically installed in many voting machines around the Nation. Many officials claim these cards are disabled in the BIOS, yet they can be re-enabled through software or firmware. When I testified alongside Tina Peters at the Colorado state capitol several years ago, urging lawmakers to physically remove these unnecessary wireless cards, the committee voted unanimously to keep them installed because they were ‘disabled in the BIOS’. If they aren’t used, then removing them altogether is the smart and safe thing to do. Yet they fought to keep them there.

The common claim that systems are “air-gapped” is equally deceptive. True physical isolation ends the moment a flash drive or any removable media is inserted, a routine practice in elections. Once that USB is plugged in, the “air-gap” is gone. Once that barrier is breached, malware or unauthorized code can easily enter.

Manipulation does not even require any connection. Sophisticated code can even be pre-installed and triggered automatically by internal conditions or even hidden signals in ballots themselves, through subtle printing defects which could be invisible to the human eye or specially crafted QR codes containing encrypted data that should not need encryption for simple ballot identification.

So how did this dangerously incomplete understanding of election security become so widely accepted? The answer lies in how the entire system is structured: a pyramid built on compromised standards, where deception flows from the top down.

Voting system vendors develop the hardware and software. They pay private testing labs to evaluate it. Those labs report their findings to the U.S. Election Assistance Commission, which

grants federal certification. States rely almost entirely on EAC certification to approve the systems. County election officials then deploy them, trusting that every level above has done its job. At the bottom of this pyramid sit the American people, whose votes ultimately depend on the integrity of the entire chain.

This system depends completely on the EAC. The agency approved VVSG 1.0 in 2005 and VVSG 1.1 in 2015, standards it later acknowledged were inadequate. In 2021 it released VVSG 2.0 to correct those deficiencies, yet it has allowed the vast majority of systems certified under the older, weaker standards to remain in use. Even VVSG 2.0 falls short, because a security standard cannot merely address most threats; it must address every credible threat vector. A single unaddressed vulnerability is enough to compromise an election.

The EAC failed to identify or close numerous critical threat vectors beyond simple internet connectivity. It failed to correct the widespread misconception it helped create. It failed the election officials who trusted its certification process and the citizens who depended on it.

In the end, the U.S. Election Assistance Commission has been fundamentally derelict in its duty. The one federal agency entrusted with protecting the integrity of our elections has let the nation down.

The phrase “not connected to the internet” was never truly about security. It was about creating and maintaining an illusion of security; an illusion that has left every American voter more vulnerable than they realize. You don’t know what you don’t know. And critically dangerous is that ‘they’ know that you don’t know what you don’t know.

The people have completely lost control of THEIR elections in

this Nation, and therefore we have an ELECTIONS NATIONAL STATE OF EMERGENCY. We must IMMEDIATELY put elections back into the hands of who they rightfully belong to, the CITIZENS. We have no time to waste; the Republic is hanging by the last thread.

Let’s fix it right now. Click here for the Declaration