A National Security Briefing on Banning Foreign-Adversary Voting Systems in U.S. Elections

What the FCC Database Reveals About the Hardware Inside U.S. Voting Systems —

Compliance Testing LLC

INTRODUCTION

This briefing presents a National Security case and clear precedent for banning foreign-adversary voting systems from U.S. elections. It is convened by Michael Schafer, CEO of Compliance Testing LLC — an ISO 17025 accredited test laboratory recognized by the Federal Communications Commission, Department of Homeland Security, Canada, and Europe — together with a small coalition of subject-matter experts.

The central facts can be verified by any reader in roughly ten minutes using nothing but public databases. Voting system manufacturers like Dominion, Sequoia, and others utilize commercial computers as their election's equipment. Many of these commercial computers including Dell, Cannon, Samsung, Fujitsu and others often include precertified wireless transmitter modules manufactured in China. The FCC certifications recorded at the FCC are under publicly searchable FCC IDs, and documented on any incorporated Transmitter module which has it's own FCC regulatory label also showing where it was manufactured and the computers are using transmitters showing "Made in China" or a "Product of China." The chain of evidence is summarized below:

- Specific computer manufacture models used in voting systems by Voting Machine Companies are publicly documented in election-office disclosures of State's Voting System inventories showing which commercial computers are used.
- The commercial computer's wireless components are documented in their public service manuals **and FCC filings.**
- Each unique wireless module transmitter carries a **unique FCC ID** number that shows, in the **FCC's public equipment-authorization database**, components with an FCC ID and include labels that require the country-of-origin for the transmitter modules (routers). These transmitter modules enable remote data connectivity of the voting systems. This kind of access can be misused in elections.

On March 23, 2026, the FCC banned foreign-produced consumer transmitters / routers and added them its "Covered List" based on National Security concerns. **The wireless modules documented inside U.S. voting Systems fall under the same National Security logic and rationale the FCC has already applied to ban "out of country" made routers.** A coalition of subject-matter experts is prepared to present the underlying evidence directly to officials with authority to assess and act on the voting systems.

EXECUTIVE SUMMARY

U.S. voting systems in current use contain China-made wireless precertified transmitter modules, under publicly searchable FCC IDs and verifiable in the FCC's own equipment-authorization database. Review of the pictures of the components below show them being made in China. The same regulatory logic and rationale the FCC ban applied on March 23, 2026 to ban foreign-produced consumer routers / transmitters from the U.S. market — for National Security concerns, a severe "supply-chain vulnerability" and "cybersecurity risk" to "critical infrastructure" — applies to these China made modules. DHS-CISA has designated U.S. voting systems used in elections as critical infrastructure. **The National Security Council has** independent authority to act in this matter. A small coalition of subject-matter experts is prepared to present the underlying evidence.

I. Foreign-Adversary Wireless Hardware Inside U.S. Voting Systems

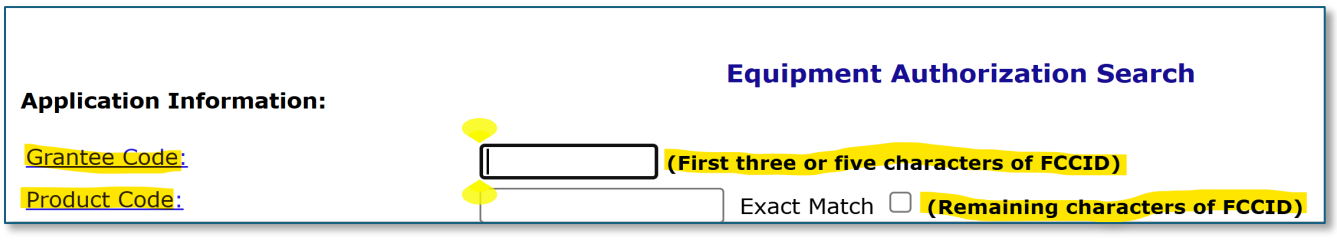
The Verifiable Supply Chain

Dominion Voting Systems and Sequoia Election Systems — the two largest U.S. voting-system providers — DO NOT manufacture the computers used as part of it's election equipment. These Voting System vendors integrate commercial off-the-shelf PCs and tablet computers as voting system devices (i.e., Dominion's documented inventory includes **Dell-branded systems OptiPlex, Latitude, Precision, and PowerEdge models**), **shipped with wireless networking modules** supplied by Intel, Realtek, Qualcomm, and Broadcom. ES&S and Sequoia equipment likewise relies on commercial PC platforms with comparable wireless options. Many of the base computers used by voting system companies contain transmitter modules. Each is an FCC-certified transmitter with its own FCC ID, its own grantee code, and its own country-of-origin disclosure on file with the Commission. The computers do not covertly add transmitting modules, it is the normal device feature anyone would buy these days. However if made by and misused a voting system could be mispurposed using foreign adversary transmitters. The risk is very serious. Serious enough for the FCC to ban foreign made routers to be used in the U.S.
https://www.fcc.gov/sites/default/files/NSD-Routers0326.pdf

The FCC Office of Engineering and Technology (OET) maintains a public database of every certified transmitter authorized for use in the United States. The database is available at **apps.fcc.gov/oetcf/eas/reports/GenericSearch.cfm**.

Entering the first three to five characters of the FCC Grantee Code into the first search field returns the official transmitter grant, the grantee, the certified frequency bands, **and the country of manufacture**.

No private access or specialized expertise is required. The search interface uses two fields: the first three to five characters of the FCC ID in the Grantee Code field; the remaining characters in the Product Code field.



Specific Modules Documented in Voting Systems

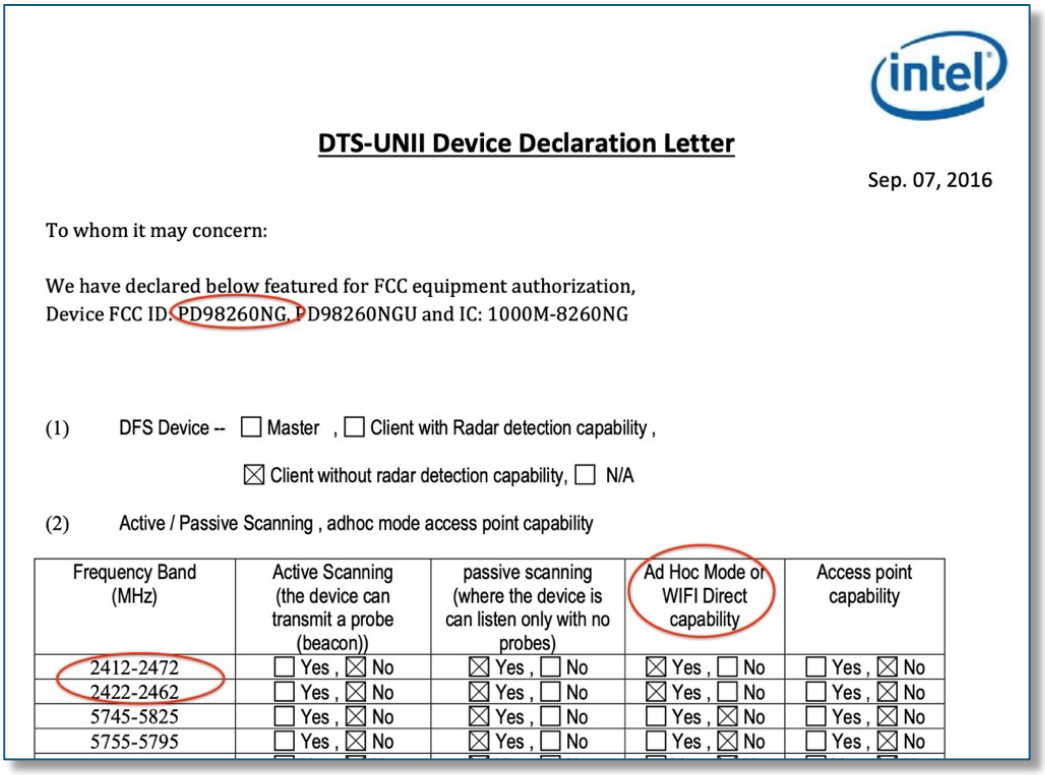
The following table lists wireless transmitter modules confirmed to be a component in the Dell models used in Dominion and other voting systems. The Dominion / Dell chain has been verified at the FCC-ID level and is documented below; the broader pattern — commercial PC platforms containing China-made FCC-certified wireless modules — applies across the U.S. voting-systems industry, including Sequoia and ES&S equipment.

Each component listed below carries an FCC ID recorded in the Commission's public equipment-authorization database to a wireless transmitter manufactured in China.

Dell Model in Voting System	Wireless Module	FCC ID (First 3 characters = Grantee Code; remainder = Product Code)	Country of Origin
Dell OptiPlex 7440 AIO	Intel Dual Band Wireless-AC 8260 (8260NGW)	PD98260NG	**Made in China**
Dell Latitude 3430	Intel Wi-Fi 6 AX201 (AX201NGW)	PD9AX201NG	**Made in China**
Dell Latitude 3430	Realtek RTL8822CE	TX2-RTL8822CE	**Made in China**
Dell Precision 3460 XE	Intel Wi-Fi 6E AX211 (AX211NGW)	PD9AX211NG	**Made in China**
Dell PowerEdge R630/R640	iDRAC Quick Sync 2 (BLE + optional Wi-Fi)	*(integrated, multiple)*	**Made in China**

*FCC equipment authorization records are publicly accessible at **fcc.gov/oet/ea/fccid**. Each FCC ID above resolves to an official grant of equipment authorization identifying the device manufacturer, country of origin, and authorized frequency bands.*

Dell and other PC manufacturers produced these platforms for general commercial use; the presence of wireless modules does not implicate them in any compliance failure. That obligation rests with the systems integrator — Dominion Voting Systems — to ensure the assembled certified voting system and accurately discloses all wireless-capable components to federal authorities and is not mispurposed.



DTS-UNII Device Declaration Letter

Sep. 07, 2016

To whom it may concern:

We have declared below featured for FCC equipment authorization, Device FCC ID: PD98260NG, PD98260NGU and IC: 1000M-8260NG

(1) DFS Device -- ☐ Master , ☐ Client with Radar detection capability , ☒ Client without radar detection capability, ☐ N/A

(2) Active / Passive Scanning , adhoc mode access point capability

Frequency Band (MHz)	Active Scanning (the device can transmit a probe (beacon))	passive scanning (where the device is can listen only with no probes)	Ad Hoc Mode or WIFI Direct capability	Access point capability
2412-2472	☐ Yes , ☒ No	☒ Yes , ☐ No	☒ Yes , ☐ No	☐ Yes , ☒ No
2422-2462	☐ Yes , ☒ No	☒ Yes , ☐ No	☒ Yes , ☐ No	☐ Yes , ☒ No
5745-5825	☐ Yes , ☒ No	☒ Yes , ☐ No	☐ Yes , ☒ No	☐ Yes , ☒ No
5755-5795	☐ Yes , ☒ No	☒ Yes , ☐ No	☐ Yes , ☒ No	☐ Yes , ☒ No

Exhibit: Intel 8260NGW FCC Declaration — Confirming Wireless Capability

*Excerpt from the official FCC equipment-authorization filing for FCC ID PD98260NG (Intel 8260NGW Wireless-AC module). The filing confirms the device's certified frequency bands and capabilities — including **Ad Hoc Mode / WiFi Direct on the 2.4 GHz band**, which allows wireless communication without a router or access point. This is the module installed in the Dell OptiPlex 7440 AIO used in Dominion voting systems. The full FCC filing is available at the FCC database link in the previous section.*

This FCC certification remains active; the 8260NGW module has continued to ship in commercial PC platforms under this same FCC ID.

Physical Evidence on the Modules Themselves

Each of the modules listed above carries its country-of-origin marking directly on its FCC regulatory label. The four photos below show the labels with red arrows highlighting the "Made in China" or "Product of China" text:



Intel 8260NGW
FCC ID: PD98260NG



Intel AX211NGW
FCC ID: PD9AX211NG

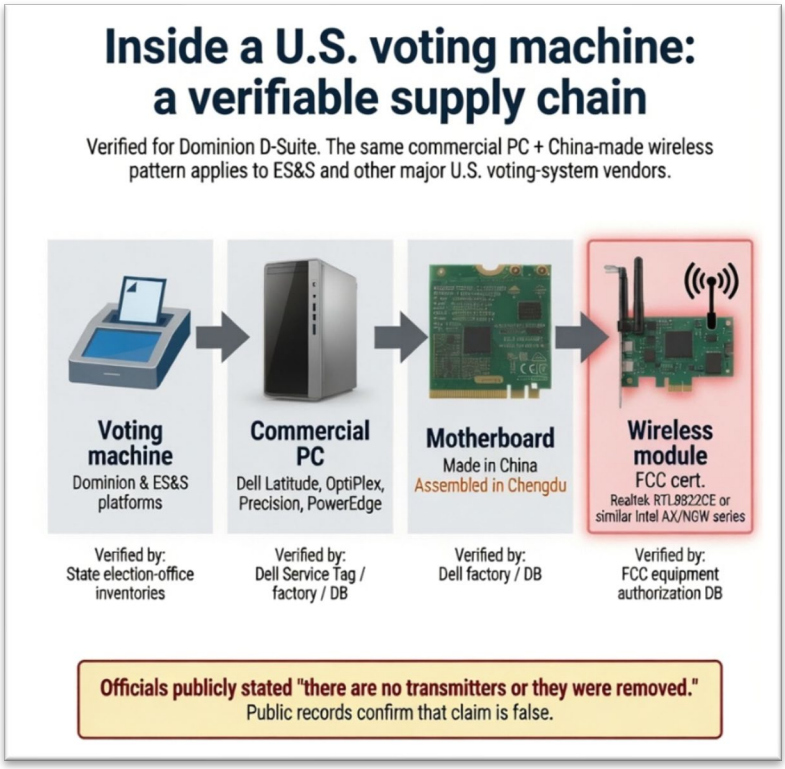


Intel AX201 (Product of China)
FCC ID: PD9AX201NG



Realtek RTL8822CE
FCC ID: TX2-RTL8822CE

Reference photos sourced from manufacturer public product imagery (Intel, Realtek). Red-arrow annotations added by the author to highlight the country-of-origin markings visible on each module's regulatory label.



The verifiable supply chain summarized: Dominion's reliance on Dell PC platforms has been verified at the FCC-ID level; the same commercial-PC + China-made-wireless pattern applies to ES&S and other major U.S. voting-system vendors.

II. The Declaration of Conformity Loophole

A reasonable reader asks: how did China-manufactured wireless transmitters end up certified for use in U.S. critical-infrastructure equipment? The answer is a specific, identifiable regulatory pathway.

Under FCC equipment-authorization rules, the system was designed for an era when supply-chain origin was not itself a National Security concern. It recently has been banned however.

The consequence: a U.S. voting machine can be marketed and deployed as “FCC-compliant” while its actual transmitter component was manufactured in a country designated as a foreign adversary under U.S. law. Compliance with the FCC certification process had not addressed the underlying supply-chain and National Security risk. Recently the FCC has banned routers not made in the U.S. for National Security concerns being addressed herein. (See Section III.)

This is a known gap in a regulatory framework that was designed before foreign-adversary supply-chain risk became a National-Security category. The gap is not the result of malicious intent on the part of any individual agency or manufacturer. But the FCC’s March 2026 router determination that non U.S. made routers present critical gaps of exactly this kind — gaps that allow foreign-adversary components to reach U.S. critical infrastructure and voting systems—and **requires immediate closure. The same recent ban standard for routers applies to voting systems.**

III. The FCC Has Already Established the Precedent for Action

On March 23, 2026, the Federal Communications Commission updated its Covered List to include all consumer-grade routers produced in foreign countries, prohibiting new FCC authorization of such devices for U.S. import or sale. The National Security Council acted on a determination by a White House-convened

Executive Branch interagency body. The reasoning the FCC adopted applies directly to the wireless modules documented in this briefing. The Commission found that foreign-produced routers / transmitters introduce:

> *"a supply chain vulnerability that could disrupt the U.S. economy, critical infrastructure, and National Security defense" and "a severe cybersecurity risk that could be leveraged to immediately and severely disrupt U.S. critical infrastructure and directly harm U.S. persons."*
>
> — FCC Fact Sheet, March 23, 2026. Full text: FCC Public Notice DA 26-278 (March 23, 2026) — Covered List Update on Foreign-Produced Routers

The Same Logic Applies to Voting-System Wireless Routers / Modules

The wireless modules documented in Section I share every relevant characteristic the FCC cited as grounds for the router ban:

- They are radio-frequency transmitters manufactured in a foreign adversary country used in U.S. voting systems.
- They reside inside equipment that DHS-CISA has designated as U.S. critical infrastructure (the nation's election systems).
- They present a supply-chain vulnerability of the exact kind the Executive Branch determination addressed.
- They are FCC-authorized devices; the FCC therefore has direct regulatory standing.

The FCC has already exercised this authority. The regulatory pathway, the rationale, the legal framework, and the precedential language all exist. All that is required is the application of the same standard to voting systems containing these precertfied router / transmitters. This is not a request that the Commission do something new or has not been done. It is a request that the Commission or another agency (perhaps the DHS) reapply what the FCC has already done.

IV. Additional Supporting Concerns

The hardware findings in Section I are sufficient to establish the National Security case. Two additional concerns warrant separate review and reinforce the same conclusion.

Voting System Software Origin is Traceable to a Foreign Adversary Design

Independent reporting and a published account in the Book Stolen Elections by author Ralph Pezzullo, draws on the firsthand account of a former CIA officer Gary Berntsen. The book documents that the core software origin now known as Smartmatic, in Sequoia, Dominion, and related voting system platforms traces to software originally designed in Venezuela to alter election outcomes. A former developer of that original software — now a U.S.-based whistleblower — could provide testimony. The coalition raises this as a parallel matter warranting review of the evidence and testimony.

Potential Conflicts of Ownership Interest in the Voting Systems Companies

Appropriate authorities should examine potential ownership stakes in Voting System companies for conflicts of interest, and improper influence via foreign adversary indirect ownership of a leading voting machine company and voting software company. Evidence and testimony can be provided.

V. Federal Agencies with Independent Authority to Act

Foreign-adversary involvement in Voting-System hardware provides grounds for action by each of the following:

1. **Federal Communications Commission (FCC):** Direct authority over equipment authorization; established precedent under the Covered List process (March 2026 router (transmitter) action).

2. **Department of Homeland Security (DHS) and CISA:** Primary authority over critical-infrastructure security; DHS-CISA has designated U.S. voting systems are critical infrastructure.

3. **Department of Commerce — Bureau of Industry & Security (BIS):** Authority over export controls and foreign-adversary technology.

4. **Department of the Treasury — Office of Foreign Assets Control (OFAC):** Authority over sanctions and financial ties to adversary nations.

5. **Department of War:** National-Security authority where adversary-controlled systems are embedded in civilian critical infrastructure. (Like the recent banning of foreign drones)

6. **Committee on Foreign Investment in the U.S. (CFIUS):** Authority to review and block foreign investment in critical technology.

VI. A Proven Alternative to Computerized Voting Systems: Easy, Fast, Accurate, Auditable Hand Counting

Removing affected voting systems is half of our election remedy. The other half already exists and has been used in the U.S. for over 100 years. Grassroots organizations have developed and field-tested fast, effective, trustworthy, accurate, auditable, repeatable hand-counting protocols. They've been used successfully in multiple elections the size of an average precinct. One well-documented reference is the Hand Count Road Show; they are trainers of hand counting elections. *(See Exhibit 2. On page 8)*

The Briefing: A Coalition Prepared to Present Testimony and Evidence

The FCC hardware findings in this briefing can be independently verified by any official with internet access in approximately ten minutes. Where deeper context is useful — the build-of-materials work behind the FCC ID and Voting System Computer Build of Materials mapping. The firsthand account of the one of the Venezuelan software's original developers, — a coalition of subject-matter experts is prepared to present that material directly.

We respectfully petition for the opportunity to convene a confidential one-day briefing with you or your designees, at a time and location of your choosing. The panel can include the technical expert who performed the component-level bill-of-materials analysis, two former SMEs familiar with election system standards and their gaps, a former developer of the Venezuelan-origin software.

About the Convener

Michael Schafer is the owner and CEO of Compliance Testing LLC, a US owned and based ISO 17025 accredited test laboratory approved and accredited for product testing by the FCC, DHS, Canada, and Europe. With more than twenty years as a subject-matter expert in electronics testing, lab accreditation and FCC, DHS and Canadian certifications of electronic devices, critical infrastructure and precertified transmitter modules testing and certification. His expertise centers on testing, accreditations, certifications, test standards and the device-certification process.

Mr. Schafer's role is as an SME and to convene the panel of experts who hold the underlying technical evidence and to translate that evidence into a simple assessment leading to banning the voting systems and to provide the regulatory understanding for the agencies with National Security authority to act similarly and consistently with the recent banning of out of country routers-transmitters.

Email: MS@ComplianceTesting.com
Phone: 480-926-1775 | 602-770-9776
Calendar: Schedule a meeting with Michael Schafer

Respectfully submitted,



Michael Schafer
CEO, Compliance Testing LLC
FCC-Accredited Test Laboratory | DHS | Canada | Europe

Exhibits — Reference Links & QR Codes



Exhibit 1 — FCC OET Equipment Authorization Search Database (verify any FCC ID)
https://apps.fcc.gov/oetcf/eas/reports/GenericSearch.cfm



Exhibit 2 — FCC Public Notice DA 26-278: Covered List Update on Foreign-Produced Routers (March 23, 2026)
https://docs.fcc.gov/public/attachments/DA-26-278A1.pdf



Exhibit 3 — CISA Advisory: Vulnerabilities Affecting Dominion Voting Systems ImageCast X
https://www.cisa.gov/news-events/ics-advisories/icsa-22-154-01



Exhibit 4 — Hand Count Road Show: Training Video & Proven Protocols
https://handcountroadshow.org/a-count-able/



Exhibit 5 — Schedule a Briefing: Michael Schafer's Calendar
https://calendly.com/michaels-compliance-testing/meetings-with-michael-schafer-day-night-40min