CONFIDENTIAL

BRIEF TO THE PRESIDENT OF THE UNITED STATES

Foreign Insider Access to United States Election Systems

*Summary of the 18 U.S.C. § 2381 Report prepared by **REDACTED** dated November 1, 2026*
Summary brief date: *November 9, 2026 prepared by **Joe Oltmann***

1. Bottom Line Up Front

Sworn testimony and internal vendor communications obtained in federal litigation establish that the engineers who built Smartmatic's election software for the Chávez and Maduro governments carried that software, its remote access architecture, and themselves from Smartmatic to Sequoia to Dominion, and today hold positions at Liberty Vote, Hart InterCivic, Smartmatic, and independent election consultancies. Those engineers built, and still operate, the VPN connections and virtual machines that reach county election management servers.

On November 3, 2020, Dominion personnel used that access in Chicago and Cook County to load, clone, split, and export results through WinEDS, a Smartmatic and Sequoia legacy server, before results reached the known official servers. The Dominion executive at the center of that work, Eric Coomer, is a former Sequoia database analyst who distributed WinEDS builds to Smartmatic's Venezuelan staff in 2006, asked Morales for a virtual machine on the Chicago VPN in March 2020, and ran the WinEDS loading in Chicago on election night. On June 14, 2022 he testified before the Fulton County special purpose grand jury whose investigation produced the indictment of President Trump that he had neither the access nor the technical capability to affect an election, and texted afterward that testifying for a grand jury investigating Trump was off his bucket list. His own emails and his 2026 deposition admissions contradict that testimony. Senior Dominion witnesses, including Coomer and Morales, denied vendor access under oath before the grand jury, in federal depositions, and in statements to the public. Dominion's chief executive, John Poulos, told Congress in January 2020 that Chinese parts were limited to commodity components, while Dominion's own records show Chinese manufactured motherboards, firmware loaded in China, and Serbian engineers modifying printer firmware with HP in Shanghai.

The federal government's own monitoring cannot see any of this. The Albert sensors deployed by CISA and the Center for Internet Security sit on the known election management server. The vendor's architecture places a second server in front of it: the HAAT Listener, a VPN repository folder, a clone, or a virtual machine. Results are processed on that first server and only the finished database is passed to the server the sensor watches. Expert review found 965 undocumented API calls into the Coffee County EMS by this route and a second, never disclosed EMS server in Maricopa County. The report's closing letter states it plainly: the engineers use unauthorized servers prior to exporting results to the known government servers, the Albert sensors and programming on the known servers will not detect the activity, and the engineers have used programming to make their exports look like normal traffic.

What is in this report is a fraction of the record. It is drawn from the Dominion discovery repository in U.S. Dominion v. Byrne and U.S. Dominion v. Powell in the United States District Court for the District of Columbia, which holds the full Coomer, Morales, Poulos, and Cardenas transcripts, the complete 2006 to 2026 email production, the Serbian and Chinese engineering correspondence, and the vendor's own network and virtual machine records. The court has sealed that repository, blocked access to it, and ordered the exhibits withdrawn from public dockets. The Department of Justice can

obtain the whole of it through its own process, and that seizure is the single step that would convert this brief from a summary of excerpts into a complete evidentiary record.

The vendor's lineage runs through a company in which the Venezuelan government held a 28 percent stake and placed its own director, that withdrew from CFIUS review rather than disclose its ownership, and whose founder is now under federal indictment in Florida. The former head of Venezuelan military intelligence has proffered that the Smartmatic system was built for the regime, exported to the United States, and has been used to alter results. The 2026 Office of the Director of National Intelligence assessment addresses none of this.

The report asks the President to direct a federal investigation of Coomer, Poulos, and Maduro's engineers for manipulation of November 3, 2020 results prior to certification and for false statements under oath, and to secure vendor remote access to election systems before it is used again.

2. Requested Action

- **Open a Department of Justice and intelligence community investigation** of Eric Coomer, John Poulos, Ronald Morales, Heider Garcia, David Moreno, Eduardo Correia, Edmundo Rojas, Alexander Soto Vasquez, Nick Ikonomakis, Xenofon Marangos, Martijn Punt, Goran Obradovic, Ranko Stamatovic, Bobana Radosavljevic, and associated Dominion, Liberty Vote, Smartmatic, and Hart InterCivic personnel for manipulation of November 3, 2020 election data prior to certification; for false statements to a grand jury, to Congress, and under oath in federal civil proceedings regarding remote access, virtual machines, Smartmatic legacy servers, and foreign programming of firmware and hardware; and for concealment of foreign ownership and foreign manufacturing from CFIUS, the Election Assistance Commission, and Congress.

- **Refer Eric Coomer.** His June 2022 grand jury testimony that he had neither the access nor the technical capability to affect an election is contradicted by his own November 3, 2020 emails, by Morales's testimony, and by his 2026 deposition admissions that he ran multiple virtual machines, that Morales may have provided one, and that Toronto, Belgrade, and Denver were connected. His 2026 testimony that absolutely no WinEDS instances were used in 2020 in any jurisdiction is contradicted by his own emails reporting WinEDS loading in Chicago that night.

- **Refer John Poulos.** His January 2020 testimony to the House Committee on Administration characterized Chinese sourcing as limited to LCD glass, capacitors, and resistors with no domestic alternative, while Dominion's records show Chinese manufactured motherboards, firmware loaded in China, and Serbian engineers modifying QR ballot printer firmware with HP in Shanghai in March 2020 on a device Dominion represented to the EAC as commercial off the shelf. His March 9, 2020 email joking about running around with a Jerry can and a box of matches, sent the day the Venezuelan machine warehouse burned, should be part of that referral.

- **Obtain the full Dominion discovery record from the District of Columbia.** Direct the Department of Justice to secure, by subpoena, search warrant, or motion to the court, the entire Dominion production and deposition record in U.S. Dominion v. Byrne, No. 1:21-cv-02131, and U.S. Dominion v. Powell, No. 1:21-cv-00040, in the United States District Court for the District of Columbia, including the sealed discovery repository, every transcript of Coomer, Morales, Poulos, and Cardenas, the complete email production, the Serbian and Chinese engineering correspondence, and the vendor's network, VPN, and virtual machine records. The excerpts in this brief are what one attorney was able to extract before the court sealed the repository and cut off her access. The remainder is sitting in that

court and only the Department can obtain it in full.

- **Fix the Albert sensor blind spot.** Direct CISA and the Center for Internet Security to map every election jurisdiction for a second server, listener, VPN repository, clone, or virtual machine that handles results before they reach the sensored EMS, to move or add sensors so that the first server is covered, and to report to the President which jurisdictions ran results through an unsensored path in November 2020, November 2024, and November 2026.

- **Preserve the November 3, 2026 systems now.** Direct that every election management server, listener server, VPN gateway, cellular modem, and vendor virtual machine used in the November 3, 2026 election be forensically imaged by federal personnel before any vendor maintenance, update, or log rotation, with specific instruction to capture both servers wherever a dual server configuration exists.

- **Order a nationwide review of vendor remote access.** Prohibit vendor VPN and virtual machine connections to county election management servers, require full logging on every network path including any second server or listener, and require disclosure to the EAC of every undocumented API such as the RemoteFileManager.Soap interface identified in Coffee County.

- **Direct the DNI to supplement the 2026 assessment** to address vendor insider threat, foreign nationals with remote access, Chinese manufacture of motherboards, and Chinese and Serbian firmware programming.

- **Pursue the Maduro connection.** Cartel de los Soles was designated a Foreign Terrorist Organization on November 16, 2025. Maduro, as Minister of Foreign Affairs from August 2006, deployed these engineers to the United States. Treat the engineers' continuing access as a foreign terrorist organization nexus and investigate accordingly.

3. Key Findings

- **Continuity of personnel.** Morales, Garcia, Moreno, Correia, Rojas, and Soto Vasquez are Venezuelan engineers who originated at Smartmatic under Chávez and Maduro. Former CNE National Director of Data Centers Wilmer Cardenas testified that Morales, Garcia, and Moreno developed Smartmatic's original election software and invented SAESdatautil, a tool that injects votes, copies election certificates, and transmits like an actual voting machine. All six remain inside the U.S. election vendor ecosystem today. Garcia additionally served as elections administrator in Placer County, California, and Tarrant and Dallas Counties, Texas, and at the U.S. Election Assistance Commission, before becoming Vice President of Customer Success at Hart InterCivic in September 2025. (Report pp. 3 to 13, 17 to 20)

- **The remote access architecture was built by Morales and came from Venezuela.** In 2007 Smartmatic Labs in Venezuela supplied Sequoia with specifications for the RAS (Remote Access Server) and the HAAT (Hybrid Activator Accumulator Transmitter) and HAAT Listener, with Morales copied. Morales testified his job was to integrate HAAT, EdgePlus, and HAAT Listener with the Sequoia WinEDS EMS sold to Chicago. Coomer testified Smartmatic created those devices and that the HAAT Listener is a separate server that receives results over a cellular network before upload into the EMS. Cardenas testified Morales configured the security network linking the United States, Canada, and Belgrade headquarters, initially by VPN, and that Serbia resolves errors in the systems during American elections. (pp. 14 to 15, 30 to 36)

- **Remote access to county servers existed in 2020 and exists now.** Morales's

emails of March 30 and 31, 2020 report a VPN connection established from a new virtual machine to reach the Chicago EMS servers, with Coomer asking for a final VM to download. Morales testified he deploys the VPN connections for voting machines in the United States along with cellular providers, that the Cook County platform had been in place for years, that an isolated connection was granted for him to reach the devices, and that unofficial results are transferred over the VPN into a server folder that the EMS reads. Coomer conceded in January and July 2026 that Toronto, Belgrade, and Denver were connected, that he believed a VPN ran from Serbia to Denver, that Morales may have given him a virtual machine during the 2020 Chicago primary, and that he had multiple virtual machines on his laptop. An August 2022 Dominion email shows Rojas and Morales among testers assigned local or remote virtual machines. (pp. 4 to 5, 16, 23, 25 to 29, 43)

- **Election night 2020 in Chicago and Cook County.** Emails dated November 3, 2020 show Coomer, Morales, Marangos, Chavez Casanova, Soto Vasquez, Obradovic, Punt, Stamatovic, Ikonomakis, McKinney, Nollette, and Smith working the early voting tally. At 12:22 AM Coomer reports a cartridge with 19,944 cards failed and that cartridges holding roughly 20,000 cards may not be readable into WinEDS. During the day he reports WinEDS loading, machines failing with out of memory errors, exporting six files, and loading the largest cartridge by itself in WinEDS. At 4:09 PM he reports that the clone is up and running. Punt describes a splitter tool that already reads result files and proposes adding the ability to write split result files, then reports successfully splitting a 12,000 ballot result file into 14 batches loaded back into RTR. McKinney asks for four exported results to be zipped and posted to the network by Tien. WinEDS is a Smartmatic and Sequoia product; a 2007 email identifies the Cook County database as residing on the WINEDS1 server. Morales testified that Marangos and Coomer provided assistance in the generation of the unofficial results that night, and Coomer testified that at times he had results in his possession and passed them to others prior to certification. (pp. 9, 11, 12, 44 to 51)

- **Eric Coomer: Sequoia, Smartmatic, and the grand jury that indicted the President.** Coomer was Senior Database Analyst at Sequoia Voting Systems in Denver in 2006, where he distributed the WinEDS 3.1.081 server build to a list that included Smartmatic's Venezuelan staff, Morales among them, while Morales was integrating Smartmatic's HAAT with the Sequoia WinEDS EMS sold to Chicago. He came to Dominion with the 2010 Sequoia acquisition and became Director of Product Strategy and Security. In March 2020 he asked Morales for a final virtual machine on the new VPN into the Chicago EMS. On November 3, 2020 he personally ran the WinEDS cartridge loading, the clone, and the result exports in Chicago. On June 14, 2022 he was called as a witness before the Fulton County Special Purpose Grand Jury, the investigation that produced the August 2023 indictment of President Trump, and testified that he did not rig the election, that he did not have the access, and that he did not have even the technical capability to compromise the security and processes needed to affect an election. The same day he texted his brother that testifying for a grand jury investigating Trump was off his bucket list. In 2026 he testified under oath that Toronto, Belgrade, and Denver were connected, that he believed a VPN ran from Serbia to Denver, that Morales may have given him a virtual machine for the 2020 Chicago primary, that he had multiple virtual machines on his laptop, that he at times had results in his possession before certification, and that absolutely no WinEDS instances were used in 2020 in any jurisdiction. His own election night emails show WinEDS loading in Chicago. His grand jury testimony was false, it was given in a proceeding aimed at the President, and the man who gave it had been working with Smartmatic's Venezuelan engineers on the same Chicago system since 2006. (pp. 16, 23, 24, 25, 31, 34, 44, 45, 47 to

49)

- **The sworn denials.** Coomer told the Fulton County grand jury on June 14, 2022 that he did not have the access and did not have even the technical capability to compromise an election, then texted that testifying for a grand jury investigating Trump was off his bucket list. He testified in 2026 that there were absolutely no WinEDS instances used in 2020 in any jurisdiction. Morales testified that Dominion employees do not use virtual machines, emphasizing not in the United States, that Dominion does not collect results data, and that he was not aware of any Dominion access to it. Dominion and Liberty Vote have maintained publicly that no Smartmatic legacy equipment or programming was used in 2020. Each statement is contradicted by the witnesses' own emails and later testimony. (pp. 2, 22, 24, 44, 52)

- **Foreign government ownership and concealment.** In 2003 the Venezuelan government's Fondo de Crédito Industrial and ANFICO formed SICR, which took 28 percent of Bizta, Smartmatic's software company, and placed government worker Omar Montilla Castillo as Bizta's director. Cardenas testified the government loaned $200,000 to develop the electoral system and that Smartmatic's president told European Union auditors in 2004 that the CNE owned the source code. In February 2004 the electoral council awarded most of a $91 million contract to Boca Raton based Smartmatic, a company whose machine had never been used in an election, after telling ES&S that the Chávez recall election would never take place. In 2006 Congresswoman Maloney twice wrote Treasury seeking CFIUS review of Smartmatic's purchase of Sequoia; Sequoia's president called Venezuelan influence a crackpot theory while a Chicago alderman traced ownership through Curaçao shell companies to Venezuelan nationals. On December 22, 2006 Smartmatic withdrew from CFIUS review and announced the sale of Sequoia rather than disclose its ownership. Antonio Mugica, the only disclosed owner, and Jorge Piñate are now under federal indictment in Florida. Maduro became Minister of Foreign Affairs in August 2006. (pp. 63 to 70)

- **Chinese hardware, Chinese firmware, Serbian programming.** Dominion's internal April 2020 email put programmable Chinese parts at 0.18 to 0.7 percent; Poulos told Congress Chinese content was LCD glass and chip level components with no domestic option. He did not disclose that motherboards are made in China. A March 24, 2020 email shows HP engineers in China and Dominion's Serbian engineers Nenad Matic and Djordje Matijevic exchanging M402 printer firmware over an FTP server while the ICX tablet sat in Shanghai customs, on a printer Dominion represented to the EAC as commercial off the shelf. Ben Cotton's hardware examination of the Image Cast Precinct found no U.S. manufactured component, Chinese high volume PCB fabrication, final assembly most likely in China, and firmware most likely loaded in China with a Chinese DFU utility, on a device fitted with an external LTE modem on its Ethernet port. Coomer testified he made no notification to CISA regarding Chinese technology used for storage in Dominion's primary data center. (pp. 25, 58 to 61)

- **The Albert sensor blind spot.** Albert sensors are the intrusion detection devices CISA and the Center for Internet Security place on election networks, and they are the basis for every federal statement that no manipulation was detected. They watch the known election management server. The vendor's architecture, as described by its own witnesses, puts a different server in front of that one. Morales testified that unofficial results travel over the VPN he deployed into a repository folder on a server from which the EMS then reads them, and that ballot images are transmitted through the Listener. Coomer testified that the HAAT Listener is a completely separate server with its own operating system that receives results before they are uploaded into the EMS. On November 3, 2020 Coomer

brought up a clone and Punt split result files into batches before they were loaded into RTR. Ben Cotton found 965 API POST calls into the Coffee County EMS through RemoteFileManager.Soap, a function absent from all EAC certification documentation, and the expert review attached to that finding states that hundreds of contacts to the EMS go undetected by Albert sensors when the contacts are received from a second server. Cotton further explains that a first server with dual network interfaces, one on the internet and one on the voting network, can be used to access the voter database, process votes, and inject tabulator data, and that if only the election database synchronizes to the second server, none of that activity exists on the server that is audited or sensored; virtual machines and virtual networks achieve the same result. Maricopa County produced only its second server to auditors after overwriting the security logs. The report's closing letter states the conclusion: the engineers use unauthorized servers prior to exporting results to the known government servers, the Albert sensors and programming on the known government servers will not detect nefarious activity, and the engineers have used programming to make their exports look like normal traffic. The federal assurance that nothing was detected is therefore an assurance about the wrong server. (pp. 34, 41, 43, 49 to 51, 55, 56, 75)

- **The sealed record in the District of Columbia.** Every deposition excerpt and vendor email in this report carries Dominion production numbers and Confidential or Highly Confidential designations from the discovery repository in U.S. Dominion v. Byrne and U.S. Dominion v. Powell before Magistrate Judge Upadhyaya in the United States District Court for the District of Columbia. That repository holds the complete record of which this brief shows fragments: the full transcripts of Coomer across three volumes, Morales, Poulos, and Cardenas; the entire Dominion email production from the Sequoia years through 2026, including the election night 2020 chains for every jurisdiction and not only Chicago; the Serbian engineering and HP China correspondence; the Wagoner virtual machine rosters; the VPN deployment records Morales testified about; and the Canton Township and Luzerne County vendor communications. After these exhibits surfaced, the court ordered them filed under seal, ordered the public filings taken down, blocked access to the repository, and removed the attorney who had produced them. The public has seen none of it, Congress has seen none of it, and the intelligence community's 2026 assessment was written without it. The Department of Justice is the only party that can obtain the whole of that record, and nothing in this brief should be read as the limit of what it contains. (pp. 2, 16, 22 to 29, 44 to 52, 59)

- **Forensic findings and evidence destruction.** Cotton reports that a Dominion ICX used in November 2020 held IP addresses resolving to the Taiwan Ministry of Education and a German cloud provider; that Fulton County's voting system had multiple networked connections and was not air gapped, including an address resolving to Carlesbourg, Canada, in the EMS client's hibernation file; that the Coffee County EMS received 965 API POST calls through RemoteFileManager.Soap, an interface absent from all EAC certification documentation; that Maricopa County had two EMS servers and produced only one to auditors after overwriting its Windows security logs; that the ICC scanner creates multiple copies of each ballot image in active memory where resident code could alter them undetected; and that vendor emails document a Dominion employee copying an election database to the internet for Serbian programmers to fix and reinsert. In March 2020, 49,408 Venezuelan voting machines holding the original Smartmatic programming burned in a CNE warehouse. On March 9, 2020 Poulos emailed Coomer, under the subject line business op, asking whether someone was running around with a Jerry can and a box of matches, Coomer replied asking where Mugica was, and Poulos replied not shady at all. Morales's own text

messages show he feared exposure of his footprints with Sequoia, Smartmatic, Premier, and Dominion, and he admitted under oath to having traveled to China. (pp. 53 to 57, 72 to 74)

4. Supporting Record
A. The engineers and their current positions

Ronald Morales
Venezuela
Dominion / Liberty Vote, Senior Systems Manager
Smartmatic QA testing in Caracas; transferred to Sequoia to integrate Venezuelan systems with U.S. equipment; built VPN and remote access; traveled to Chicago with Correia and Piñate
2, 3, 17, 21, 23, 26 to 28, 32 to 43, 46, 74
Heider Garcia
Venezuela
Hart InterCivic, VP of Customer Success (Sep 2025)
Smartmatic 2003 to 2016; Placer County CA Elections Manager; Tarrant County TX Elections Administrator; U.S. EAC Senior Subject Matter Expert (2023); Dallas County TX Elections Administrator (2023 to 2025)
6, 18, 19
David Moreno
Venezuela
The Canton Group, Group Product Manager, Election Technology
Smartmatic Caracas and Mexico 2001 to 2006; Sequoia 2006 to 2010; Dominion PM 2010 to 2012; Dominion Sr. Director Election Production and Testing 2020 to 2024; logged urgent Luzerne County PA request on Jan 6, 2021
7, 17, 18, 19
Eduardo Correia
Venezuela
Smartmatic, Chief Technology Officer
Smartmatic since 2003, Caracas then Panama; EAC certified Smartmatic's U.S. system to VVSG 2.0 on Dec 2, 2025; traveled to Chicago with Morales
8, 19, 21
Edmundo Rojas
Venezuela
Liberty Vote, Senior Product Specialist (contract)
University of Technology Venezuela, Caracas; Dominion on site services and L and A testing; assigned Dominion testing virtual machine Aug 2022
4, 5, 29
Alexander Soto Vasquez
Venezuela
ASV Global Solutions, founder (Oct 2026)
Liberty Vote Customer Success Manager Sep 2019 to Apr 2026; led Chicago election technology environment, 5,500 devices; Puerto Rico and Mongolia deployments; on Nov 3, 2020 Coomer emails
10, 11
Nick Ikonomakis
Canada
Dominion / Liberty Vote, VP Engineering (since 2008)
Dominion since 2003; on Nov 3, 2020 Coomer emails
9
Bobana Radosavljevic
Serbia
Dominion / Liberty Vote, Product Owner
QA Analyst 2018 to 2020; on Oct 30, 2020 McKinney email about WinEDS batch sizes for Chicago early voting
12
George Poulos
Canada
Liberty Vote, Software Engineer, Denver
Dominion intern in Belgrade 2023 implementing AES and 3DES smart card encryption; Dominion intern in Toronto 2022
13

Cardenas testified that any technician who has worked in Smartmatic and had contact with the source code knows all its vulnerabilities and can use that knowledge for whatever they want, and that Morales was transferred from Smartmatic to Sequoia when Smartmatic bought Sequoia

specifically to integrate the Venezuelan systems with the American systems. (pp. 14, 15)

B. Origin of the remote access architecture, 2003 to 2010

- Cardenas testified that the same Smartmatic solutions team that built the Venezuelan system developed WinEDS, used in the 2006 Chicago election in which Senator Obama voted on a Smartmatic machine; that the Venezuelan SAES 3200 became the U.S. SAES 3367; that Venezuela was the test case for the 2006 U.S. election; that iterations were made by the Sequoia team of Garcia, Morales, and Moreno; and, asked whether the tool can change the results of an election, answered totally. (p. 18)

- Cardenas testified that [SAES data util] injects votes into the electoral system, copies libraries, holds the election certificates and the permits for transmitting data, and that after Smartmatic's 2007 platform refresh only Smartmatic could use it. Asked whether Morales, Victor Vasquez, Edmundo, and Moreno had access to the tool, he answered that they developed it and invented it. (pp. 19, 20)

- On August 1 and 2, 2007 Fernando Hernández of Smartmatic Labs, Venezuela, sent Sequoia's Chris York the hardware and software specifications for the HAAT Listener servers and the RAS Server, including the instruction to enable and configure the RRAS remote access service, with Morales copied. (pp. 30, 31)

- Morales testified that in 2006, while employed by Smartmatic, he worked with Sequoia to integrate the HAAT, the EdgePlus, and the HAAT Listener with the Sequoia EMS called WinEDS and the Insight machine, and that his work in Chicago was to make sure equipment for both companies worked together. He tested the HAAT and later improved its hardware. He testified the Listener acts as a bridge between the HAAT and a repository folder on a server where transmitted information is stored. (pp. 32, 33, 35, 36)

- Coomer testified in Coomer v. Byrne on January 27, 2026 that Smartmatic created the Edge2 Plus and the HAAT, that WinEDS and Smartmatic developed protocols to share information, and that the HAAT Listener is a completely separate server with a different operating system that receives results over a segregated cellular network, after which results are uploaded, usually via sneakernet, into the central EMS. A 2018 Stamatovic email states that once election results are sent through the internet from tabulators or RTM the system is not closed any more. (pp. 31, 34)

- A December 22, 2006 email from Coomer, then Senior Database Analyst at Sequoia, distributed an updated WinEDS 3.1.081 server build to a list that included Smartmatic addresses. An April 18, 2007 email from Chris York states that the Cook County database resides on the WINEDS1 server, gives its login and password, and states that the HAAT files were changed so they will work in Denver. (pp. 23, 47)

C. Remote access, VPN, and virtual machines, 2020 and after

- Morales, March 30, 2020, to Nollette and Coomer, subject VPN access with City: we were able to establish a VPN connection from the new virtual machine created today, and tomorrow we will work toward the changes that allow us to reach the EMS servers from the VPN connection. Coomer, March 31, 2020: do we have an updated ETA on completion and a final VM I can at least download. (p. 23)

- Morales testified that he works in the deployment of the connections established for the VPN for the voting machines, along with the cellular providers; that the Cook County platform and VPN had been in place for years before the November 3, 2020 election; and that his access was an isolated connection granted for him to connect to those devices. (pp. 26 to 28)

- Morales testified that unofficial results are transferred to the VPN and stored in a folder on the server so the EMS can come and read them. The United States certifies elections on those unofficial electronic results; many states require recounts on the same tabulators. (p. 43)

- Coomer, January 27, 2026: there were connections between Toronto and Denver, and Belgrade and Denver; the Dominion Denver office exists. He also described a contingency VPN into a city server that was configured but, he testified, never enabled. (p. 16)

- Coomer, July 10, 2026, Vol. III: Morales potentially gave him a virtual machine; Ronald may have provided one as a backup during the 2020 Chicago primary, I believe he did; asked whether there was a VPN from Serbia to Denver, I believe so; I had multiple virtual machines on my laptop. He made no notification to CISA regarding Chinese technology used for storage in the Dominion primary data center. (p. 25)

- Jerry Wagoner, Dominion Director of Technical Services, August 10 to 12, 2022: testers for Democracy Suite 5.17 are issued local or remote virtual machines from a Dominion share; the roster includes Edmundo Rojas and Ronald Morales; access to the virtual VM is granted on request. (pp. 5, 29)

D. Election night, November 3, 2020, Chicago and Cook County

- October 30, 2020, McKinney to Coomer, Punt, Soto Vasquez, Marangos, Smith, copying Ikonomakis, Obradovic, Radosavljevic, Vukovic, Stamatovic, Milovanovic: Chicago loads early voting tabulator results Monday night; set the batch size in WinEDS to 5 to 10 for early voting and raise it to 50 to 75 as polls close. (p. 12)

- November 3, 2020, 12:00 and 12:22 AM, Coomer to Smith, Chavez Casanova, Marangos, Morales, Soto Vasquez, copying McKinney, Obradovic, Punt, Stamatovic, Nollette, Ikonomakis, importance high: cartridge 31057 with 19,944 cards failed after 55 minutes; we may have a situation; we already have several cartridges with roughly 20,000 cards cast and may not be able to read these results into WinEDS. McKinney: the largest early voting cartridge in the primary had 5,736 ballots; now I am wide awake. (pp. 9, 11, 47)

- November 3, 2020, Coomer: exporting the six files took four minutes; WinEDS loading; two of three machines failed with out of memory exceptions; I am now trying to load the largest cartridge we have by itself in WinEDS; otherwise we will have to rescan upwards of 20,000 cards as a catastrophic fallback; all early voting cards have been copied to the NAS; RTR loading of the remaining 47 cartridges; this is for the City, Cook will be very time constrained. (p. 48)

- November 3, 2020, 9:24 AM, Coomer; then Punt: the splitter tool that splits the mapping XML already reads the result files, I believe we could add writing of split result files as well, taking a single ICP result file and saving it as multiple ICC result files, because ICC can have multiple batches; we will integrate this in the current splitter tool as a proof of concept. (p. 50)

- November 3, 2020, 3:04 PM, McKinney to Coomer, Nollette, Soto Vasquez, copying Morales, Punt, Smith, Marangos, Obradovic, Stamatovic, Ikonomakis, Chavez Casanova: any chance you can zip those four exported results up and have Tien post to the network. 10:08 PM: I guess I would also need the mapping file. Punt: we successfully used the tool to split a 12,000 result file into 14 ICC batches that were then loaded back into RTR; results matched; we can provide this tool to Mark. (p. 51)

- November 3, 2020, 4:02 PM, Nollette: was the restore of the Cook image on

the city side successful. 4:09 PM, Coomer: we just got the clone up and running, trying to load the 7300 ballot cartridge, memory usage spiked to 2 GB. (p. 49)

- Morales testified that Smith was the account manager for Cook County and that Marangos and Coomer were more in the providing of assistance to the customer in the generation of the unofficial results on election night, while he monitored the hardware. Coomer testified that at times he had results in his possession and passed them to someone else prior to certification of the election. (pp. 45, 46)

- Morales testified that Cook County needed to transfer ballot images from the machines to the main system, the EMS, and that customers with the Listener decide what they want to transmit. Asked who at Dominion sought certification of the software change allowing ballot images to be transmitted through the Listener, he answered that certification was not his role. (p. 41)

- November 4, 2020, Anthony Essmaker, Deputy Clerk, Charter Township of Canton, Michigan: tabulator AVCB 2 batch 151 was to be deleted by Dominion but ended up in the final results; it was a duplicate batch they thought was removed earlier in the day but showed up in RTR; Dominion walked us through it on the EMS. This shows the vendor's ability to remove and restore batches within results files. (p. 53)

E. Eric Coomer: from Sequoia and Smartmatic to the Fulton County grand jury

Dec 22, 2006
Coomer, Senior Database Analyst, Sequoia Voting Systems, 1800 Glenarm Place, Denver, sends the updated WinEDS 3.1.081 server build and release notes to a distribution list that includes morales@smartmatic.com, Miguel Botto, Fernando Hernández, and other Smartmatic Venezuela staff. Coomer is listed as the assignee on the fixed defects.
23
2006 to 2007
Morales, then at Smartmatic, integrates the HAAT, Edge Plus, and HAAT Listener with the Sequoia WinEDS EMS sold to Chicago. Sequoia's York notes the HAAT files were changed so they will work in Denver, where Coomer worked, and that the Cook County database resides on the WINEDS1 server.
32, 35, 47
2010
Dominion acquires Sequoia. Coomer continues and becomes Director of Product Strategy and Security. Morales and Moreno move with him.
2, 7, 23
Mar 31, 2020
Coomer to Morales and Nollette: do we have an updated ETA on completion and a final VM I can at least download, in reply to Morales's report that a VPN from a new virtual machine would reach the Chicago EMS servers.
23
Nov 3, 2020
Coomer runs WinEDS loading in Chicago, reports cartridge failures and out of memory errors, loads the largest cartridge by himself in WinEDS, exports six files in four minutes, brings the clone up, and is on every email in which Punt proposes writing split result files and McKinney asks for exported results to be zipped and posted to the network.
9, 11, 47 to 51
Nov 3, 2020
Morales later testifies that Marangos and Coomer were providing assistance to the customer in the generation of the unofficial results on election night.
46
June 14, 2022
Coomer testifies before the Fulton County Special Purpose Grand Jury, the investigation that produced the August 2023 Fulton County indictment of President Trump. Asked whether he rigged the election: no, I didn't, and nor would I even be able to. I don't have the access. Dominion just builds the hardware and provides the software, we do not run elections. Nor do I have even the technical capability to compromise all of the security and processes that are in place that would be needed to affect an election.
24
June 14, 2022
Coomer texts: testifying for a grand jury investigating Trump is off my bucket list; some jurors actually asked good questions. Bill Coomer: that is good news.

24
Jan 27, 2026
Coomer v. Byrne deposition: there were connections between Toronto and Denver, and Belgrade and Denver; Smartmatic created the Edge2 Plus and HAAT; WinEDS and Smartmatic developed protocols to share information; the HAAT Listener is a separate server receiving results over a cellular network before upload into the EMS.
16, 31, 34
July 10, 2026
Coomer Vol. III deposition: Morales potentially gave him a virtual machine, and may have provided one as a backup during the 2020 Chicago primary; asked about a VPN from Serbia to Denver, I believe so; I had multiple virtual machines on my laptop; no CISA notification regarding Chinese storage technology in Dominion's primary data center.
25
July 10, 2026
Coomer Vol. III deposition: there were absolutely no WinEDS instances used in 2020 in any jurisdiction; it was one of the big goals of the company to migrate all customers off WinEDS by 2020; asked whether that occurred, not for 100 percent, no. Elsewhere: one redacted jurisdiction used the Sequoia system post 2010 and I cannot remember when we migrated it to the full Dominion ecosystem.
44
Undated
Coomer deposition: asked whether he had results in his possession, in his hand, passing to somebody else, prior to certification of the election: at times, yeah, maybe. Yes.
45

The grand jury testimony on access and technical capability was material to the investigation of the President, because Dominion's assertion that its personnel could not touch the vote was the premise on which claims of manipulation were treated as baseless. The record above shows that Coomer had remote access through a VPN and virtual machines, had personally handled results on election night through a Smartmatic legacy server, and had worked alongside Smartmatic's Venezuelan engineers on that very system since 2006. The report asks that Coomer be investigated for false testimony before the grand jury, for false testimony in federal depositions, and for his role in the November 3, 2020 handling of results prior to certification.

F. Sworn denials contradicted by the record

Coomer, Fulton County Special Purpose Grand Jury, June 14, 2022
I don't have the access. Nor do I have even the technical capability to compromise the security and processes needed to affect an election.
His Nov 3, 2020 emails loading, cloning, and exporting Chicago results; 2026 admissions of multiple VMs, a VM from Morales, Serbia to Denver VPN; Morales's testimony that Coomer assisted in generating results.
24, 25, 46, 48, 49
Coomer, deposition, July 10, 2026
There were absolutely no WinEDS instances used in 2020 in any jurisdiction. Did not use WinEDS during the 2020 election.
His own Nov 3, 2020 emails reporting WinEDS loading and failures in Chicago; Oct 30, 2020 email setting WinEDS batch sizes; his own testimony that one jurisdiction stayed on the Sequoia system after 2010 and he cannot remember when it migrated.
12, 44, 47, 48
Coomer, deposition, January 27, 2026
I wasn't connected to anything in Denver.
Same deposition: there were connections between Toronto and Denver, and Belgrade and Denver.
16
Morales, U.S. Dominion v. Powell, July 25, 2024
Does any county use virtual machines to host Dominion software: No. Not in the United States, no.
His March 30 and 31, 2020 emails establishing a VPN from a new virtual machine to the Chicago EMS; Aug 2022 Dominion VM roster listing him; Coomer's testimony that Morales gave him a VM.
22, 23, 25, 29
Morales, same deposition
Dominion doesn't collect any of that data; Dominion has no access to results that I'm aware of.
His testimony that unofficial results transfer over the VPN he deployed into a server folder; Nov 3, 2020 emails exporting and splitting result files; Coomer's possession of results before certification.
43, 45, 48 to 52
Morales, same deposition
No HAAT, no Listener, no Smartmatic or Sequoia products in Chicago in 2020.

WinEDS, the Sequoia and Smartmatic EMS, was in use in Chicago on Nov 3, 2020 per the vendor's own emails; Cook County data resided on the WINEDS1 server.
40, 47, 48
Poulos, House Committee on Administration, January 2020
Chinese content is LCD glass and chip level capacitors and resistors; no option for U.S. manufacture.
Chinese manufactured motherboards; firmware loaded in China; HP Shanghai firmware exchange with Serbian engineers; no U.S. component on the ICP.
58 to 61
Dominion and Liberty Vote, public statements
No Smartmatic legacy equipment or programming was used in 2020.
Everything above.
2

G. Foreign government ownership and control

- 1999 to 2003: the Fondo de Crédito Industrial, an autonomous entity of the Venezuelan Ministry of Finance, and ANFICO formed Sociedad de Inversión Capital de Riesgo Venezuela, SICR, also called SCR. On December 15, 2003 SCR subscribed 300 million bolívares of new shares in Bizta R and D Software, with Eduardo Correia Nascimento, Alfredo Anzola, Antonio Mugica Rivero, and Antonio Mugica Sesma as the other shareholders, giving the government 28 percent. Omar Montilla Castillo, a government worker, was named a director of Bizta. (pp. 67 to 69)

- Cardenas testified the Venezuelan government loaned $200,000 to develop the electoral system, that CNE director Jorge Rodríguez's contract negotiation required Montilla's placement at Bizta, and that in the 2004 European Union audit Mugica stated that the CNE owned the source code and gave Smartmatic permission to keep using it. (p. 69)

- April 2004, Miami Herald: Rodríguez told ES&S that the recall election would never take place and asked whether ES&S worked for the CIA; the council instead awarded most of a $91 million contract to Boca Raton based Smartmatic, whose touch screen machine had never been used in an election anywhere. (p. 70)

- May 4 and October 6, 2006: Congresswoman Carolyn Maloney wrote Treasury Secretaries Snow and Paulson seeking CFIUS review of Smartmatic's acquisition of Sequoia, noting the Venezuelan government's 28 percent stake, Mugica as the only disclosed owner, Smartmatic's ownership hidden through offshore entities, the HAAT software at issue in Chicago, and Sequoia bringing Venezuelan nationals to work the Chicago 2006 primary. Maduro was appointed Minister of Foreign Affairs by Chávez in August 2006. (pp. 63, 65)

- April 8, 2006, Chicago Tribune: Sequoia president Jack Blaine called Venezuelan influence a crackpot theory and flatly denied Chávez was pulling strings, while Alderman Burke traced ownership through Curaçao shell companies to Venezuelan nationals and said the city may have stumbled across an international conspiracy to subvert the electoral process. (p. 64)

- December 22, 2006: Smartmatic announced it would sell Sequoia and withdraw from CFIUS review. Smartmatic was also reported at that time to be the subject of a Department of Justice investigation into bribery of the Venezuelan government and tax fraud. The report characterizes this as the plan to launder the Smartmatic and Sequoia identity. Dominion acquired Sequoia in 2010 and the same people and programming moved with it. (pp. 2, 66)

- December 2, 2025: Hugo Carvajal Barrios, former Director of Military Intelligence of Venezuela, proffered in a letter to the President that Smartmatic was born as an electoral tool of the regime, that he placed the head of IT at the CNE who reported to him,

that the system can be altered, that the technology was later exported abroad including to the United States, that regime operatives maintain relationships with election officials and voting machine companies inside the United States, and that he states with certainty elections can be rigged with the software and it has been used to do so. (p. 71)

- November 16, 2025: Secretary Rubio designated Cartel de los Soles, also known as Cartel of the Suns, a Foreign Terrorist Organization under Section 219 of the INA. Carvajal identifies the organization as the Chávez government turned criminal enterprise now run by Maduro, Cabello, and senior regime officials. (pp. 2, 71)

H. Supply chain: China and Serbia

- April 2020 internal Dominion emails prepared responses to congressional questions for the record stating that 0.18 to 0.7 percent of programmable electronic parts are sourced from China. Poulos told the House Committee on Administration that Chinese components were LCD glass and chip level capacitors and resistors with no option for U.S. manufacture. (p. 58)

- March 24, 2020, Lu Yu Chun of HP to Nenad Matic of Dominion, copying Djordje Matijevic of Dominion and HP engineers in China: the M402 printer firmware for USTATUS changes is ready and uploaded to the FTP server; the tablet is at Shanghai customs awaiting clearance. Dominion represented the printers to the EAC as commercial off the shelf. (p. 59)

- Hardware report dated July 11, 2025, edited March 16, 2026, on the PCOS 320 ImageCast Precinct: components from Epson, Sharp, Sanyo, STMicroelectronics, Microchip, ON Semiconductor, Realtek, and SMSC, all fabricated in China, Taiwan, Malaysia, Thailand, or the Philippines; silkscreen and PCB characteristics consistent with Chinese high volume fabrication; no UL or U.S. fabrication tags; chassis typical of Chinese contract manufacturing; final assembly approximately 96 percent likely China; firmware loading likely China with a Chinese DFU utility; date codes week 45 and 46 of 2015 consistent with the Democracy Suite 4.14 E rollout; contract manufacturers likely Flex, Pegatron, Wistron, or Jabil; U.S. EMS companies found to be only regional offices coordinating Asian production. The subject unit carried an external LTE modem connected to its Ethernet port. (pp. 60, 61)

- Poulos never disclosed to Congress that motherboards are made in China or that Serbian employees work with a Chinese vendor to modify firmware, which the report states subverts U.S. government oversight of the Chinese and Serbian programming. (p. 59)

I. Forensic findings (Ben Cotton, November 1, 2026)

- Antrim County, Michigan: the forensic image of a Dominion ICX used in November 2020 contained IP address 120.125.201.101, resolving to the Ministry of Education Computer Center in Taipei, Taiwan, within a TCP/IP socket configuration, and IP address 62.146.7.79, resolving to a German cloud provider. The device was configured on a private 10.114.192.x network with FTP settings and had communicated with public IP addresses outside the United States. (p. 57)

- Fulton County, Pennsylvania: multiple networked connections external to the voting system network, indicating the system was not air gapped, including 172.102.27.194, resolving to a provider in Carlesbourg, Canada, found in the hibernation file of EMS Client01. (p. 57)

- Coffee County, Georgia: 965 API POST calls to the EMS via RemoteFileManager.Soap. No API documentation of any such function appears in the EAC

certification documentation. Contacts arriving from a second server go undetected by Albert sensors. (p. 55)

- Maricopa County, Arizona: two EMS servers existed; the county produced only one to Senate auditors after overwriting all Windows security logs for the election period; the other server was never disclosed. A first server with dual network interfaces can be used for remote access, vote processing, and injection of tabulator data while only the election database synchronizes to the second server, so that no trace of unauthorized access appears on the server produced for audit. Virtual machines and virtual networks achieve the same result. Vendor emails document a Dominion employee copying an election database to the internet where Serbian programmers fixed it before reinsertion into the EMS. (p. 56)

- ICC and Adjudication: memory analysis shows multiple copies of each scanned ballot created in active memory, presenting the opportunity for memory resident programs to modify one or more images without detection; the scanner is programmed to create duplicate ballot copies, allowing modification of final results files. (p. 54)

J. Evidence destruction and consciousness of guilt

- Cardenas was National Director of Data Centers at the CNE and before that responsible for the warehouse and distribution of over 48,000 voting machines across Venezuela. The report states those machines, from the contested 2018 election, contained evidence of nefarious programming and tally manipulation. (p. 72)

- March 2020: the CNE's main warehouse burned, destroying 49,408 voting machines, 582 civil registry computers, and 400 electronic ballots. (pp. 72, 73)

- March 9, 2020, Poulos to Coomer, subject business op: running around with a Jerry can and a box of matches, lol. Coomer: where was Mugica. Poulos: not shady at all. (p. 73)

- Morales, in messages read into his deposition: at least the list of Venezuelans in Chicago in 2006 has now disappeared; they left me with all the footprints with Sequoia, Smartmatic, Premier equipment, and Dominion; I thought I was one of the safest because I did not have any exposure. Asked whether he has been to China, he answered yes. (p. 74)

- Mugica and Piñate are under federal indictment in Florida. Morales acknowledged under oath that he, Correia, and Piñate traveled from Venezuela to Chicago to provide assistance, and that he learned years later from a coworker of a list of Venezuelan employees who traveled to Chicago to assist with elections. (pp. 21, 73)

K. The Albert sensor blind spot: the unsensored first server

- What the sensors watch. Albert sensors are network intrusion detection appliances provided through CISA and the Center for Internet Security to state and county election offices. They are installed on the network segment of the known election management server. Federal statements since 2020 that no manipulation was detected rest on these sensors and on the logs of that server.

- What sits in front of them, in the vendor's own words. Coomer, January 27, 2026: the HAAT Listener is a completely separate server with a different operating system that receives results over a segregated cellular network, after which results are uploaded into the central EMS. Morales: unofficial results are transferred to the VPN and stored in a folder on the server so the EMS can come and read them; Cook County transfers ballot images through the Listener; he deployed the VPN connections and customers decide what to transmit; nobody at Dominion sought certification for the change that allowed ballot images through the Listener. Stamatovic, 2018: once election results are sent through the internet

from tabulators or RTM, the system is not closed any more. (pp. 34, 41, 43)

- What happened on that first server on November 3, 2020. Coomer brought up a clone and loaded cartridges into it. Punt modified the splitter tool to write split result files and split a single 12,000 ballot result file into 14 ICC batches that were then loaded back into RTR. McKinney had exported results zipped and posted to the network. All of this occurred before results were loaded into the system of record. (pp. 49 to 51)

- Cotton, Coffee County, Georgia: 965 API POST calls to the EMS via RemoteFileManager.Soap, with no API documentation of any such function or capability in any EAC certification documentation. The expert review attached to that statement: hundreds of contacts to the Election Management System go undetected by Albert sensors when the contacts are received from a second server. (p. 55)

- Cotton, the dual server mechanism: a first server for remote access using dual home network interfaces, one network with internet access and the other on the voting system network. Unauthorized personnel can access the Server 1 voter database, process votes, inject new tabulator data, and perform other voting administrative functions. If the only data synchronized with the second server is the election database, none of the unauthorized accesses from Server 1 would exist on Server 2. If only Server 2 is provided for an audit, none of the unlawful activities and access would be present. The same skirting of auditing and detection can be accomplished using virtual machines and virtual networks. None of the system logs from Server 1 would be on Server 2. (p. 56)

- Cotton, Maricopa County, Arizona: two EMS servers existed; the county provided only one to the Senate auditors after overwriting all of the Windows system security logs; the logs that remained did not include user logins, security events, or remote access authentication for the 2020 election period; the other server was never disclosed or produced. Vendor emails document a Dominion employee copying the election database out to the internet, Serbian programmers fixing it, and the fixed database being reinserted into the EMS. (p. 56)

- The report's conclusion, page 75: the engineers use unauthorized servers prior to exporting results to the known government servers. The Albert sensors, and programming on the known government servers, will not detect nefarious activity. The engineers have used programming to make their exports look like normal traffic. (p. 75)

Taken together: the sensor is on the second server, the vendor's foreign engineers hold VPN and virtual machine access to the first, results are processed and reshaped on the first, and only the finished database reaches the sensored machine. A federal finding of no detected manipulation is a finding about a server the manipulation never has to touch.

L. The sealed record in the District of Columbia and what DOJ seizure would yield

- Where the exhibits come from. The deposition excerpts, vendor emails, virtual machine rosters, and HP firmware correspondence in this report bear Dominion production numbers and Confidential and Highly Confidential designations. They were produced by Dominion in discovery in U.S. Dominion v. Byrne, No. 1:21-cv-02131, and U.S. Dominion v. Powell, No. 1:21-cv-00040, in the United States District Court for the District of Columbia, and held in an online repository under an Amended Protective Order of June 16, 2023 before Magistrate Judge Moxila Upadhyaya.

- What the court did when the exhibits surfaced. In March 2024 the court ordered the Dominion material filed under seal, ordered the exhibits withdrawn from public dockets, blocked the producing attorney's access to the repository, and in August 2024

removed her from the case. The public, Congress, the Election Assistance Commission, and the Office of the Director of National Intelligence have not had access to the repository. The 2026 DNI assessment was written without it.

- What the repository holds that this brief does not. The complete Coomer transcripts across three volumes in 2026 and his earlier testimony; the complete Morales, Poulos, and Cardenas transcripts; the full Dominion email production from the Sequoia period through 2026, of which the Chicago chains on November 3, 2020 are one jurisdiction on one night; the Belgrade and Toronto engineering correspondence; the HP China firmware exchange in full; the Wagoner virtual machine assignment records; the VPN deployment records Morales testified he maintains; the Canton Township and Luzerne County vendor communications; and Dominion's own internal responses to the congressional questions for the record on Chinese sourcing.

- Why only the Department of Justice can get it. The protective order binds every private party who has touched the material and the court has shown it will sanction disclosure. A federal criminal process, by subpoena, search warrant, or motion for access in aid of a criminal investigation, is not bound by the civil protective order and can obtain the repository, the depositions, and the native files with metadata intact. That single step converts this brief from excerpts into a complete evidentiary record and removes the question of how the material was obtained.

- What to ask for specifically. The full repository with production logs; all deposition transcripts and video; all native email with headers; the Dominion network diagrams, VPN configurations, and virtual machine inventories produced or withheld on privilege; the Chicago, Cook County, Coffee County, Maricopa, Antrim, Fulton County Pennsylvania, Canton Township, and Luzerne County vendor communications; and the privilege logs, so that withheld items can be reviewed by the Department rather than by Dominion.

M. Deficiencies in the federal assessment

National Intelligence Council memorandum NICM 2020 003 of January 15, 2020, declassified by DNI Gabbard on March 16, 2026, assesses that Russia, China, Iran, and North Korea have the capability to access election related systems, but states that vote tabulation systems would be difficult to manipulate because they are not connected to the internet. The report marks this as false and notes the assessment fails to address insider vendor access, Chinese manufactured motherboards, phone chips, and modified firmware for QR ballot printers. The report asks that the deficiency be corrected. (p. 62)

5. Exhibit Index by Report Page

2
Federal Register, FTO designation of Cartel de los Soles, Nov 16, 2025
Establishes the Maduro network as a designated terrorist organization
3
Cardenas summary; list of eight engineers
Frames the insider threat
4 to 5
Rojas LinkedIn; Wagoner VM emails Aug 2022
Current Liberty Vote employee with Dominion VM access
6
Garcia LinkedIn
Smartmatic to county administrator to EAC to Hart InterCivic
7
Moreno LinkedIn; Vukovic Jan 6, 2021 email
Smartmatic to Sequoia to Dominion; Luzerne County PA
8
Correia LinkedIn; EAC VVSG 2.0 certification Dec 2, 2025
Smartmatic CTO; Smartmatic certified for U.S. use
9
Ikonomakis RocketReach; Nov 3, 2020 12:22 AM Coomer email
Canadian VP Engineering on the election night chain
10 to 11
Soto Vasquez LinkedIn; same Coomer email
Chicago lead now independent vendor
12
Radosavljevic LinkedIn; Oct 30, 2020 McKinney WinEDS email
Serbian engineer; WinEDS batch settings for Chicago
13
George Poulos LinkedIn
Belgrade intern now Liberty Vote engineer in Denver
14 to 15
Cardenas transcript on three headquarters, VPN, Morales
Remote access network built by Morales
16
Coomer v. Byrne, Jan 27, 2026, pp. 124, 252
Toronto, Belgrade, Denver connected; contingency VPN
17
Cardenas on Morales and Moreno
Original Smartmatic developers; software used to rig Venezuela
18
Cardenas p. 25
WinEDS built by same team; Chicago 2006; tool can change results
19 to 20
Cardenas p. 24 and SAESdatautil
Vote injection tool invented by Morales, Vasquez, Edmundo, Moreno
21
Morales, Powell depo, p. 61
Chicago travel with Piñate and Correia
22, 52
Morales depo
Denies VMs in U.S.; denies Dominion access to results
23
Morales VPN emails Mar 30 to 31, 2020; Coomer Dec 2006 WinEDS build
VPN from VM to EMS; Smartmatic on Sequoia build list
24
Fulton grand jury transcript June 14, 2022; Coomer texts
Denial of access and capability
25
Coomer Vol. III, July 10, 2026
Multiple VMs; VM from Morales; Serbia VPN; Chinese storage
26 to 28

Morales depo
Deployed VPN; in place for years; isolated connection
29
Wagoner emails Aug 2022
Tester VM roster including Rojas and Morales
30 to 31
Hernández and York emails Aug 2007; Coomer p. 187
RAS and HAAT specifications from Venezuela
32 to 33, 35 to 36
Morales depo p. 305 and following
Integrated HAAT with WinEDS; Listener as bridge
34
Stamatovic 2018 email; Coomer p. 292
Not a closed system; HAAT Listener as separate server
37 to 40
Morales depo
Denies HAAT, Listener, Smartmatic, Sequoia products in 2020
41
Morales depo p. 232
Ballot images transmitted through Listener; certification evaded
42
Morales depo p. 245
QA testing of Smartmatic EMS in Caracas
43
Morales depo
Unofficial results over VPN to server folder
44
Coomer depo
Denies WinEDS in 2020 in any jurisdiction
45
Coomer depo
Possessed results prior to certification
46
Morales depo p. 286
Marangos and Coomer generating results on election night
47
Nov 3, 2020 emails; York Apr 18, 2007 email
WinEDS loading; Cook database on WINEDS1 server
48
Coomer Nov 3, 2020 email
WinEDS loading, export, NAS, RTR
49
Nov 3, 2020 4:02 and 4:09 PM emails
Clone up and running; Cook image restore
50 to 51
Punt and McKinney Nov 3, 2020 emails
Splitter tool; zipped results posted to network
53
Canton Township MI Nov 4, 2020 email
Dominion deletion of batches from results
54
Cotton statement Nov 1, 2026
ICC creates duplicate ballot images in memory
55
Cotton statement Nov 1, 2026 and expert note
965 undocumented API calls to Coffee County EMS; Albert sensors miss contacts from a second server
56
Cotton statement Nov 1, 2026; Maricopa audit cover
Dual server mechanism defeats audit and detection; Serbian fix of election database
57
Cotton Antrim and Fulton reports
Foreign IP addresses; not air gapped
58
Poulos congressional transcript; Dominion QFR emails Apr 2020
Chinese parts testimony
59

HP Shanghai firmware email Mar 24, 2020
Serbian and Chinese firmware modification
60 to 61
PCOS 320 hardware report
No U.S. component; firmware loaded in China
62
NICM 2020 003, declassified Mar 16, 2026
DNI assessment deficient
63, 65
Maloney letters May 4 and Oct 6, 2006
CFIUS inquiry; 28 percent Venezuelan stake
64
Chicago Tribune Apr 8, 2006
Sequoia denials; Curaçao ownership trail
66
Maloney press release Dec 22, 2006
Smartmatic withdraws from CFIUS; sells Sequoia
67 to 69
SICR charter; Bizta shareholder minutes Dec 15, 2003; Cardenas p. 11
Venezuelan government ownership and director
70
Miami Herald Apr 20, 2004
$91 million contract; recall will never take place
71
Carvajal proffer letter Dec 2, 2025
Smartmatic exported to U.S. and used to rig
72 to 73
Cardenas p. 9; warehouse fire Mar 10, 2020; Poulos and Coomer emails Mar 9, 2020
Evidence destroyed; matches joke; Mugica
74
Morales depo
Footprints; travel to China
75
Closing letter to the President
Unauthorized servers before the known government server; Albert sensors will not detect; exports made to look like normal traffic; investigation requested

6. Note

The exhibits in this brief are excerpts from Documentum and a sealed discovery repository in the District of Columbia case of Dominion v Byrne et al.