Premier Election Solutions

From Wikipedia, the free encyclopedia

Premier Election Solutions, formerly **Diebold Election Systems, Inc.** (**DESI**),[1] was a subsidiary of Diebold that made and sold voting machines.

In 2009, it was sold to competitor ES&S. In 2010, Dominion Voting Systems purchased the primary assets of Premier, including all intellectual property, software, firmware and hardware for Premier's current and legacy optical scan, central scan, and touch screen voting systems, and all versions of the GEMS election management system from ES&S.

At the time ES&S spun off the company due to monopoly charges its systems were in use in 1,400 jurisdictions in 33 states and serving nearly 28 million people.[2]

Premier Election Solutions

Formerly	Diebold Election Systems, Inc.
Company type	Subsidiary
Industry	Electronic Voting hardware Consulting
Founded	January 22, 2002; 23 years ago (as Diebold Election Systems) Ohio, U.S.
Fate	Acquired by Dominion Voting Systems
Headquarters	North Canton, Ohio, U.S.
Products	AccuVote-TSX, AccuVote-OS, AccuView Printer Module, Global Election Management System (GEMS), DIMS-NeT, ExpressPoll-2000, ExpressPoll-4000, VoteRemote Suite
Website	Premier Election Solutions

History [edit]

DESI was run by Bob Urosevich, starting in 1976. In 1979, Bob Urosevich founded, and served as the president (through 1992) of, *American Information Systems*, now known as Election Systems & Software, Inc. (ES&S), becoming a chief competitor to DESI. Todd Urosevich, Bob's brother, was vice president, aftermarket sales, of Election Systems & Software, Inc.

In 1995, Bob Urosevich started I-Mark Systems, whose product was a touch screen voting system utilizing a smart card and biometric encryption authorization technology. Global Election Systems, Inc. (GES) acquired I-Mark in 1997, and on 31 July 2000, Bob Urosevich was promoted from Vice President of Sales and Marketing and New Business Development, to president and chief operating officer. On January 22, 2002, Diebold announced the acquisition of GES, then a manufacturer and supplier of electronic voting terminals and solutions. The total purchase price, in stock and cash, was $24.7 million. Global Election Systems subsequently changed its name to Diebold Election Systems, Inc.[*citation needed*]

ne change [edit]

In late 2006, Diebold decided to remove its name from the front of the voting machines in what its spokesperson called "a strategic decision on the part of the corporation".[3] In August 2007 Diebold Election Systems changed its name to "Premier Election Solutions" ("PES").[1]

Acquisition by Election Systems & Software [edit]

Election Systems & Software (ES&S) acquired Premier Election Solutions on September 3, 2009. ES&S President and CEO Aldo Tesi said combining the two companies would result in better products and services for customers and voters.[4]

Acquisition by Dominion [edit]

Following the acquisition, the Department of Justice and 14 individual states launched investigations into the transaction on antitrust grounds.[5] In March 2010, the Department of Justice filed a civil antitrust lawsuit against ES&S, requiring it to divest voting equipment systems assets it acquired from Premier Election Solutions in order to restore competition.[6] The company sold the assets to Dominion Voting Systems.

Dominion Voting Systems acquired Premier on May 19, 2010.[7] "We are extremely pleased to conclude this transaction, which will restore much-needed competition to the American voting systems market and will allow Dominion to expand its capabilities and operational footprint to every corner of the United States," said John Poulos, CEO of Dominion. The transaction was approved by the Department of Justice and nine state attorneys general.[8]

Controversies [edit]

O'Dell's fundraising [edit]

In August 2003, Walden O'Dell, chief executive of Diebold, announced that he had been a top fundraiser for President George W. Bush and had sent a get-out-the-funds letter to Ohio Republicans. In the letters he said he was "committed to helping Ohio deliver its electoral votes to the president next year."[9] Although he clarified his statement as merely a poor choice of words, critics of Diebold and/or the Republican party interpreted this as at minimum an indication of a conflict of interest, at worst implying a risk to the fair counting of ballots. He responded to the critics by pointing out that the company's election machines division is run out of Texas by a registered Democrat. Nonetheless, O'Dell vowed to lower his political profile lest his personal actions harm the company. O'Dell resigned his post of chairman and chief executive of Diebold on December 12, 2005, following reports that the company was facing securities fraud litigation surrounding charges of insider trading.[10]

Security and concealment issues [edit]

> *For more information on the 2004 elections see: 2004 United States election voting controversies: Voting machines*

In January 2003, Diebold Election Systems' proprietary software, and election files, hardware and software specifications, program files, voting program patches, on its file transfer protocol site, were leaked, later 7 August 2003 leaked to *Wired*.[11] [12][13][14][15]

In 2004, Avi Rubin, a professor of computer science at Johns Hopkins University and Technical Director of the Information Security Institute, analyzed the source code used in these voting machines and reported "this voting system is far below even the most minimal security standards applicable in other contexts."[16][17] Following the publication of this paper, the State of Maryland hired Science Applications International Corporation (SAIC) to perform another analysis of the Diebold voting machines. SAIC concluded "[t]he system, as implemented in policy, procedure, and technology, is at high risk of compromise."[18]

In January 2004, *RABA Technologies*, a security company in Columbia, Maryland, did a security analysis of the Diebold AccuVote, confirming many of the problems found by Rubin and finding some new vulnerabilities.[19][20]

In June 2005, the *Tallahassee Democrat* reported that when given access to Diebold optical scan vote-counting computers, Black Box Voting, a nonprofit election watchdog group founded by Bev Harris, hired Finnish computer expert Harri Hursti and conducted a project in which vote totals were altered, by replacing the memory card that stores voting results with one that had been tampered with. Although the machines are supposed to record changes to data stored in the system, they showed no record of tampering after the memory cards were swapped. In response, a spokesperson for the Florida Department of State said, "Information on a blog site is not viable or credible."[21]

In early 2006, a study for the state of California corroborated and expanded on the problem;[22] on page 2 the California report states that:

"Memory card attacks are a real threat: We determined that anyone who has access to a memory card of the AV-OS, and can tamper it (i.e. modify its contents), and can have the modified cards used in a voting machine during election, can indeed modify the election results from that machine in a number of ways. The fact that the results are incorrect cannot be detected except by a recount of the original paper ballots" and "Harri Hursti's attack does work: Mr. Hursti's attack on the AV-OS is definitely real. He was indeed able to change the election results by doing nothing more than modifying the contents of a memory card. He needed no passwords, no cryptographic keys, and no access to any other part of the voting system, including the GEMS election management server."

A new vulnerability, this time with the TSx DRE machines, was reported in May 2006. According to Professor Rubin, the machines are "much, much easier to attack than anything we've previously said... On a scale of one to 10, if the problems we found before were a six, this is a 10. It's a totally different ballgame."[23][24] According to Rubin, the system is intentionally designed so that anyone with access can update the machine software, without a pass code or

AccuVote-TSx DRE voting machine with VVPAT attachment, at right

other security protocol. Diebold officials said that although any problem can be avoided by keeping a close watch on the machines, they are developing a fix.[25]

Michael I. Shamos, a professor of computer science at Carnegie Mellon University who is a proponent of electronic voting and the examiner of electronic voting systems for Pennsylvania, stated "It's the most severe security flaw ever discovered in a voting system." Douglas W. Jones, a professor of computer science at the University of Iowa, stated "This is the barn door being wide open, while people were arguing over the lock on the front door." Diebold spokesman David Bear played down the seriousness of the situation, asserting that "For there to be a problem here, you're basically assuming a premise where you have some evil and nefarious election officials who would sneak in and introduce a piece of software. I don't believe these evil elections people exist."[26]

On October 30, 2006, researchers from the University of Connecticut demonstrated new vulnerabilities in Diebold AccuVote-OS optical scan voting terminal. The system can be compromised even if its removable memory card is sealed in place.[27]

On September 13, 2006, Director of the *Center for Information and Technology Policy*[28] at Princeton University, Professor Edward Felten, and graduate students Ariel Feldman and Alex Halderman discovered severe security flaws in a Diebold AccuVote-TS voting machine.[29][30] Their findings claimed, "Malicious software running on a single voting machine can steal votes with little if any risk of detection. The malicious software can modify all of the records, audit logs, and counters kept by the voting machine, so that even careful forensic examination of these records will find nothing amiss."[31][32][33][34][35]

On November 2, 2006, HBO premiered *Hacking Democracy*, a documentary about the vulnerability of electronic voting machines (primarily Diebold) to hacking and inaccurate vote totals. The company argued that the film was factually inaccurate and urged HBO to air a disclaimer explaining that it had not verified any of the claims.[36][37][38] However, corroboration and validation for the exploits shown in *Hacking Democracy* was published in a report for the state of California (see above).

In January 2007, a photo of the key used to open Diebold voting machines was posted in the company's website. It was found possible to duplicate the key based on the photo. The key unlocks a compartment which contains a removable memory card, leaving the machine vulnerable to tampering.[39]

A report commissioned by Ohio's top elections official on December 15, 2007, found that all five voting systems used in Ohio (made by Elections Systems and Software; Premier Election Solutions (formerly Diebold Election Systems); and Hart InterCivic) have critical flaws that could undermine the integrity of the 2008 general election.[40]

On July 17, 2008, Stephen Spoonamore made the claim that he had "fresh evidence regarding election fraud on Diebold electronic voting machines during the 2002 Georgia gubernatorial and senatorial elections." Spoonamore is "the founder and until recently the CEO of Cybrinth LLC, an information technology policy and security firm that serves Fortune 100 companies." He claims that Diebold Election Systems Inc. COO Bob Urosevich personally installed a computer patch on voting machines in two counties in Georgia, and

that the patch did not fix the problem it was supposed to fix.[41] Reports have indicated that then Georgia Secretary of State Cathy Cox did not know the patch was installed until after the election.[42]

States rejecting Diebold [edit]

In 2004, after an initial investigation into the company's practices, Secretary of State of California Kevin Shelley issued a ban on one model of Diebold voting machines in that state. California Attorney General Bill Lockyer, joined the state of California into a false claims suit filed in November 2003 by Bev Harris and Alameda County citizen Jim March.[43][44]

The suit charged that Diebold had given false information about the security and reliability of Diebold Election Systems machines that were sold to the state. To settle the case, Diebold agreed to pay $2.6 million and to implement certain reforms.[45] On August 3, 2007, California Secretary of State Debra Bowen decertified Diebold and three other electronic voting systems after a "top-to-bottom review of the voting machines certified for use in California in March 2007."[46]

In April 2007, the Maryland General Assembly voted to replace paperless touchscreen voting machines with paper ballots counted by optical scanners, effective in time for the 2010 general (November) elections. The law, signed by the Governor in May 2007, was made contingent on the provision of funding by no later than April 2008. The Governor included such funding in his proposed budget in January 2008,[47] but the funding was defeated by the state House in July 2008.[48]

In March 2009, California Secretary of State Debra Bowen decertified Diebold's GEMS version 1.18.19 after the Humboldt County Election Transparency Project discovered that GEMS had silently dropped 197 ballots from its tabulation of a single precinct in Eureka, California.[49] The discovery was made after project members conducted an independent count using the ballot counting program Ballot Browser.

Leaked memos [edit]

In September 2003, a large number of internal Diebold memos, dating back to 1999, were posted to the BlackBoxVoting.org web site, resulting in the site being shut down due to a Diebold cease and desist order. Later, other website organizations Why War? and the Swarthmore Coalition for the Digital Commons, a group of student activists at Swarthmore College posted the memos. U.S. Representative Dennis Kucinich, a Democrat from Ohio, placed portions of the files on his websites.[50]

Diebold attempted to stop the publication of these internal memos by sending cease-and-desist letters to each site hosting these documents, demanding that they be removed. Diebold claimed the memos as their copyrighted material, and asserted that anyone who published the memos online was in violation of the Online Copyright Infringement Liability Limitation Act provisions of the Digital Millennium Copyright Act found in §512 of the United States Copyright Act.

When it turned out that some of the challenged groups would not back down, Diebold retracted their threat. Those who had been threatened by Diebold then sued for court costs and damages, in *OPG v. Diebold*. This

suit eventually led to a victory for the plaintiffs against Diebold, when in October 2004 Judge Jeremy Fogel ruled that Diebold abused its copyrights in its efforts to suppress the embarrassing memos.

Stephen Heller [edit]

In January and February 2004, a whistleblower named Stephen Heller brought to light memos from Jones Day, Diebold's attorneys, informing Diebold that they were in breach of California law by continuing to use illegal and uncertified software in California voting machines. California Attorney General Bill Lockyer filed civil and criminal suits against the company, which were dropped when Diebold settled out of court for $2.6 million. In February 2006, Heller was charged with three felonies for this action.[51][52] On November 20, 2006, Heller made a plea agreement to pay $10,000 to Jones Day, write an apology, and receive three years probation.[53]

Diebold and Kenneth Blackwell's conflict of interest [edit]

Ohio State Senator Jeff Jacobson, Republican, asked Ohio Secretary of State Ken Blackwell, also a Republican, in July 2003 to disqualify Diebold's bid to supply voting machines for the state, after security problems were discovered in its software, but was refused.[54] Blackwell had ordered Diebold touch screen voting machines, reversing an earlier decision by the state to purchase only optical scan voting machines which, unlike the touch screen devices, would leave a "paper trail" for recount purposes. Blackwell was found, in April 2006, to own 83 shares of Diebold stock, down from 178 shares purchased in January 2005, which he attributed to an unidentified financial manager at Credit Suisse First Boston who had violated his instructions to avoid potential conflict of interest, without his knowledge.[55] When Cuyahoga county's primary was held on May 2, 2006, officials ordered the hand-counting of more than 18,000 paper ballots after Diebold's new optical scan machines produced inconsistent tabulations, leaving several local races in limbo for days and eventually resulting in a reversal of the outcome of one race for state representative. Blackwell ordered an investigation by the Cuyahoga County Board of Elections; Ohio Democrats demanded that Blackwell, who was also the Republican gubernatorial candidate in 2006, recuse himself from the investigation due to conflicts of interest, but Blackwell did not do so.[56]

The Republican head of the Franklin County, Ohio Board of Elections, Matt Damschroder, said a Diebold contractor came to him and bragged of a $50,000 check he had written to Blackwell's "political interests."[57]

See also [edit]

- Black box voting
- ChoicePoint
- Electoral fraud
- 2018 United States elections (2018 Georgia elections)[58]

References [edit]

1. ^ a b "Diebold Election Systems to Become Premier Election Solutions" (Press release). Diebold Election

Systems, Inc. August 16, 2007. Archived from the original on June 6, 2011. Retrieved March 26, 2021.
2. ^ "Dominion Voting Systems, Inc. Acquires Premier Election Solutions Assets From ES&S". Benzinga.com. Archived from the original on November 13, 2020. Retrieved November 22, 2011.
3. ^ Barney Gimbel, Fortune writer-reporter (November 3, 2006). "Rage against the machine: Diebold struggles to bounce back from the controversy surrounding its voting machines (Fortune, 3. November 2006)". Money.cnn.com. Retrieved November 22, 2011.
4. ^ "ES&S buys competitor". Omaha World-Herald (Omaha.com). Archived from the original on September 8, 2012. Retrieved March 9, 2009.
5. ^ Ben Klayman (December 19, 2009). "U.S. opens probe of Diebold unit sale -report". Thomson Reuters. Retrieved January 20, 2010.
6. ^ United States Department of Justice (March 8, 2010). "Justice Department Requires Key Divestiture in Election Systems & Software/Premier Election Solutions Merger". Retrieved November 9, 2012.
7. ^ "Dominion Voting Systems, Inc. Acquires Premier Election Solutions Assets From ES&S". *Business Wire*. May 20, 2010. Retrieved November 9, 2012.[*permanent dead link*]
8. ^ "Archived copy" (PDF). Archived from the original (PDF) on July 4, 2010. Retrieved 2010-11-11.
9. ^ Paul Krugman (December 2, 2003). "Hack The Vote". *The New York Times*. Retrieved June 21, 2012.
10. ^ Lundin, Leigh (August 17, 2008). "Dangerous Ideas". *Voting Fiasco, Part 279.236(a)*. Criminal Brief. Retrieved October 7, 2010.
11. ^ Manjoo, Farhad (September 23, 2003). "An open invitation to election fraud". *Salon.com*. Archived from the original on October 9, 2003.
12. ^ McWilliams, Brian (August 7, 2003). "New Security Woes for E-Vote Firm". *Wired News*. Archived from the original on October 8, 2003.
13. ^ Harris, Bev (February 5, 2003). "BREAKING NEWS: Voting System Integrity Flaw". *Scoop News*. Archived from the original on October 2, 2003. Retrieved June 6, 2021. "Diebold Election Systems, which builds the AccuVote machines, both optical scan and touch-screen, was parking files on an unprotected public Internet location. Not a few files – thousands of files; election files, hardware and software specifications, program files, voting program patches – and sometimes, files with curious names."
14. ^ "The research and activism arm of BlackBox Voting.com". *BlackBoxVoting.org*. Archived from the original on July 13, 2003.
15. ^ BlackBoxVoting.org (September 26, 2003). "Diebold Demands Pull-Down of Black Box Voting". Talion.com: Red Dog Publicity & inexpensive PR support. Archived from the original on September 27, 2003.
16. ^ Kohno, T.; A. Stubblefield; A. D. Rubin; D. S. Wallach (2004). "Analysis of an electronic voting system". *IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004* (PDF). pp. 27–40. CiteSeerX 10.1.1.100.4963. doi:10.1109/SECPRI.2004.1301313. ISBN 978-0-7695-2136-7. ISSN 1081-6011. S2CID 12203239.
17. ^ Rubin, Aviel David (September 5, 2006). *Brave New Ballot: The Battle to Safeguard Democracy in the Age of Electronic Voting*. Broadway. p. 288. ISBN 978-0-7679-2210-4.
18. ^ Archived version of State of Maryland's Risk Assessment Report regarding Diebold AccuVote-TS Voting System and Processes. Archived on August 27, 2006. Retrieved January 6, 2009.
19. ^ "Trusted Agent Report Diebold AccuVote-TS Voting System, RABA Innovative Solution Cell (RiSC)" (PDF). March 25, 2004. Archived from the original (PDF) on May 12, 2008. Retrieved November 22, 2011.

20. ^ Guernsey, Lisa (September 16, 2004). "Holding the Vote-Counting Machines Accountable" . *The New York Times*. Retrieved June 6, 2021. "What about other attempts at tampering? In a simulation last year, a team of experts with RABA Technologies, a security company in Columbia, Md., attempted to hack into the cards by guessing passwords. The team was able to gain access to the cards' contents after a few guesses and create a forged supervisor card. With such a card, a perpetrator could disable a touch-screen unit."
21. ^ "Tests in Leon County, Florida, Demonstrate Ease of Vote Count Hacking" . *Reclaim Democracy!*. Reclaimdemocracy.org. June 4, 2005. Retrieved September 17, 2021.
22. ^ "Security Analysis of the Diebold AccuBasic Interpreter "
23. ^ Hacker House (March 18, 2021). "election hacking" . *GitHub*. Retrieved June 6, 2021. "Useful tools and configuration files for injecting your own code into a Diebold AccuVote TSx system. To make use of these utilities you will need an OpenOCD compatible debugger such as the TinCanTools FlySwatter 2. You will also benefit from a PCMCIA to CompactFlash adapter and NE2000-based ethernet PCMCIA card. You need to ensure that you get a compatible card, you can then load your own EXE or ROM onto the Diebold AccuVote TSx system. You can also make use of the flash memory to make your adjustments permenant [*sic*]."
24. ^ "Election Machine Hacking: Diebold AccuVote-TSx Runs 'Space Invaders' " . *Hacker House*. October 24, 2019. Retrieved June 6, 2021.
25. ^ Experts see new Diebold flaw: They call it worst security glitch to date in state's voting machines and a 'big deal' TMCnet.com, May 12, 2006
26. ^ New Fears of Security Risks in Electronic Voting Systems New York Times, May 12, 2006. Also see Security Focus in depth four page report.
27. ^ Security Assessment of the Diebold Optical Scan Voting Terminal Archived May 10, 2008, at the Wayback Machine (UConn VoTeR Center and Department of Computer Science and Engineering, University of Connecticut, October 30. 2006)
28. ^ "Home" . *Center for Information Technology Policy*. Princeton, New Jersey: Princeton University. Archived from the original on October 31, 2007. Retrieved June 6, 2021.
29. ^ Schulberg, Jessica (July 17, 2017). "Good News For Russia: 15 States Use Voting Machines That Have Been Easily Hackable For More Than A Decade" . *HuffPost*. Retrieved June 6, 2021.
30. ^ POTTER, NED (September 15, 2006). "Elections Easy to Steal, Say Computer Scientists" . *ABC News*. Retrieved June 6, 2021.
31. ^ Ariel J. Feldman; J. Alex Halderman; Edward W. Felten (September 13, 2006). "Security Analysis of the Diebold AccuVote-TS Voting Machine" (PDF). Princeton University. Archived from the original (PDF) on May 13, 2007. Retrieved May 7, 2007. `{{cite journal}}`: Cite journal requires `|journal=` (help)
32. ^ Feldman, Ariel J.; Halderman, J. Alex; Felten, Edward W. (September 13, 2006). "Security Analysis of the Diebold AccuVote-TS Voting Machine" . *Center for Information Technology Policy*. Archived from the original on December 12, 2017. Retrieved June 6, 2021.
33. ^ CITP Princeton (November 30, 2016). "Security Demonstration of DieBold AccuVote-TS Electronic Voting Machine" . via: YouTube. Archived from the original on December 12, 2021. Retrieved June 6, 2021.
34. ^ CITP Princeton (December 1, 2016). "Access to Diebold AccuVote-TS Electronic Voting Machine – close up" . via: YouTube. Archived from the original on December 12, 2021. Retrieved June 6, 2021.
35. ^ CITP Princeton (December 1, 2016). "Access Diebold AccuVote-TS Electronic Voting Machine – angle view" . via: YouTube. Archived from the original on December 12, 2021. Retrieved June 6, 2021.
36. ^ "Cease and Desist letter from Diebold Elections' President David Byrd" (PDF). Archived from the original (PDF) on October 18, 2011. Retrieved November 22, 2011.
37. ^ Michael Janofsk (October 31, 2006). "Seattle PI story on the Diebold press release regarding 'Hacking Democracy' " . Seattlepi.com. Retrieved November 22, 2011.

38. ^ Clarke, Gavin (November 2, 2006). "Article from 'The Register' regarding Diebold's letters to HBO" . Theregister.co.uk. Retrieved November 22, 2011.
39. ^ Diebold shows how to make your own voting machine key .
40. ^ Driehaus, Bob (December 15, 2007). "Ohio Elections Official Calls Machines Flawed (Published 2007)" . *The New York Times*. Archived from the original on June 10, 2021.
41. ^ "The Raw Story – GOP cyber-security expert suggests Diebold tampered with 2002 election" . *rawstory.com*. Archived from the original on April 25, 2017.
42. ^ "The Raw Story – Documents show Georgia's Secretary of State knew of Diebold patch" . *rawstory.com*.
43. ^ "copy of case number RG031284 Archived February 18, 2012, at the Wayback Machine"
44. ^ "Vote machine maker settles over her whistle-blower suit "
45. ^ Gimbel, Barney (November 3, 2006). "Rage against the machine" . *Fortune Magazine*.
46. ^ "Top-To-Bottom Review" . California Secretary of State. August 3, 2007. Archived from the original on August 17, 2007. Retrieved August 10, 2007.
47. ^ "TrueVote Applauds O'Malley For Funding Transition to Paper Ballot" . VoteTrustUSA. January 16, 2008. Retrieved August 15, 2008.
48. ^ Michael Hardy (July 16, 2008). "House defeats paper ballot funding" . FCW.com. Archived from the original on August 4, 2008. Retrieved August 15, 2008.
49. ^ "Withdrawal of Approval of GEMS 1.18.19" (PDF). State of California Secretary of State. March 30, 2009. Archived from the original (PDF) on June 27, 2009.
50. ^ "Kucinich Calls for Suspension of Electronic Voting Archived March 3, 2016, at the Wayback Machine," *Common Dreams*, April 23, 2004.
51. ^ So, Hemmy (March 18, 2006). "Whistle-Blower or Thief in Diebold Case?" . *Los Angeles Times*. Retrieved July 14, 2009.
52. ^ "Stephen Heller Legal Defense Fund - Oakland Tribune article" . *www.hellerlegaldefensefund.com*. Archived from the original on December 28, 2006.
53. ^ "[dead-link] Los Angeles County District Attorney's Office statement regarding Stephen Heller's plea bargain" . November 28, 2007. Archived from the original on November 28, 2007. Retrieved November 22, 2011.
54. ^ "Voting Machine Controversy" . Commondreams.org. August 28, 2003. Archived from the original on February 4, 2012. Retrieved November 22, 2011.
55. ^ "Improper stock buy reported" . Vindy.com. April 4, 2006. Archived from the original on October 13, 2016. Retrieved November 22, 2011.
56. ^ Democrats want Blackwell to remove himself from election probe Canton Repository, May 9, 2006
57. ^ "Vendor's donation questioned" . *Columbus Dispatch*. July 16, 2005.[*dead link*]
58. ^ Vasquez, Christan; Choi, Matthew (November 5, 2018). "Voting machine errors already roil Texas and Georgia races" . *Politico*.

External links [edit]

- Official website
- Official site of Diebold-Procomp Brazil
- Official site of Dominion Voting

Research and reports [edit]

- Security Analysis of the Diebold AccuVote-TS Voting Machine , Princeton University

- Analysis of an Electronic Voting System , Avi Rubin at Johns Hopkins University
- The Case of the Diebold FTP Site by Douglas W. Jones, Professor of Computer Science at the University of Iowa
- voting_system_report by Science Applications International Corporation
- Maryland Voting Systems Study , RTI International, December 2, 2010
- Top-to-Bottom Review of voting systems by the government of California
- Online Policy Group v. Diebold case file from Electronic Frontier Foundation
- Diebold takes down blackboxvoting.org , Egan Orion, *The Inquirer*, September 24, 2003
- Con Job at Diebold Subsidiary , *Associated Press*, Wired, December 17, 2003

Categories: 2010 mergers and acquisitions | 2004 United States election voting controversies | Diebold | Election technology companies | Electronic voting companies | Stark County, Ohio