CRITICAL INFRASTRUCTURE SUBSECTOR	Election Systems
SUBJECT	Internet Connectivity
COMPONENT SCOPE	Election Management Systems
RISK LEVEL	High
ELECTION RECORDS IMPACTED	All election records

1 Introduction

Internet connections to/from components within an election system compromise the security of elections. Physical transfers of election records such as post-election results are secured with the application of configuration-controlled seals and bipartisan signatories. In contrast, digital transfers of election records such as post-election results occur regularly without any bipartisan oversight and are often performed/shared with Non-Government Organizations (NGO) not subject to any substantive public oversight at all. In order for the general public to trust the integrity of election outcomes, it is imperative that digital record transfers using internet connections feature security protocols commensurate with the precautions used for physical data transfers.

2 Background

Electronic voting system vendors often assert that their systems are “air-gapped” implying no internet connectivity. There is evidence, however, to suggest that many election systems feature internet connections hidden from election officials.

2.1 Connection Types

Digital election record transfers can be conducted via any one of the following connection types:

- Ethernet
- Wi-Fi
- Bluetooth Tether
- Cellular
- Transfer to/from Portable Digital Storage Device (e.g. USB Flash Drive)

2.2 Security Protocols

In order to secure the transfer of digital election records using all but the digital storage device method, the following security protocols provide enhanced but not absolute security:

- Account Security
- Encryption
- Virtual Private Networks
- Zero Trust Tunnels

The transfer of digital records via a Portable Digital Storage Device is typically secured via the same security protocols used for physical records.

2.3 Internet Connectivity Evidence

Before November 3, 2020, the observation that electronic voting systems were connected to the internet was widely accepted as fact. After November 3, 2020, there was a significant censorship campaign implemented against anyone re-asserting this fact. Despite these censorship efforts, the evidence is clear that our election systems are indeed still connected to the internet.

2.3.1 Center for Internet Security

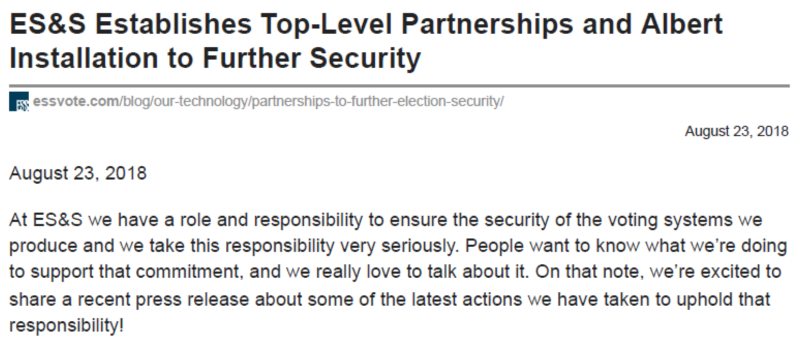
Perhaps the clearest indicator that our election systems use internet connections is the fact that the Department of Homeland Security (DHS) contracted the Center for Internet Security (CIS) to manage the Election Integrity Information Sharing and Analysis Center (EI-ISAC). Their primary means of securing election systems is via the installation of Albert Sensors and associated software to assist in the management of network traffic.

2.3.2 ES&S

Election Systems & Software (ES&S) is the nation's largest electronic voting system vendor controlling approximately 50% of the U.S. Market.

2.3.2.1 CIS Partnership

ES&S openly acknowledges their partnership with CIS via their promotion of Albert Sensor installations intended to secure internet-based communications.



ES&S Establishes Top-Level Partnerships and Albert Installation to Further Security

essvote.com/blog/our-technology/partnerships-to-further-election-security/

August 23, 2018

August 23, 2018

At ES&S we have a role and responsibility to ensure the security of the voting systems we produce and we take this responsibility very seriously. People want to know what we're doing to support that commitment, and we really love to talk about it. On that note, we're excited to share a recent press release about some of the latest actions we have taken to uphold that responsibility!

Figure 1 ES&S Bulleting Announcing CIS Partnership

2.3.2.2 Hidden Cellular Modems

One of the court exhibits provided in the William Bailey v Antrim County, MI lawsuit featured the revelation of a hidden 4G modem from Tellt Systems installed on the motherboard of an ES&S DS 200 tabulator.

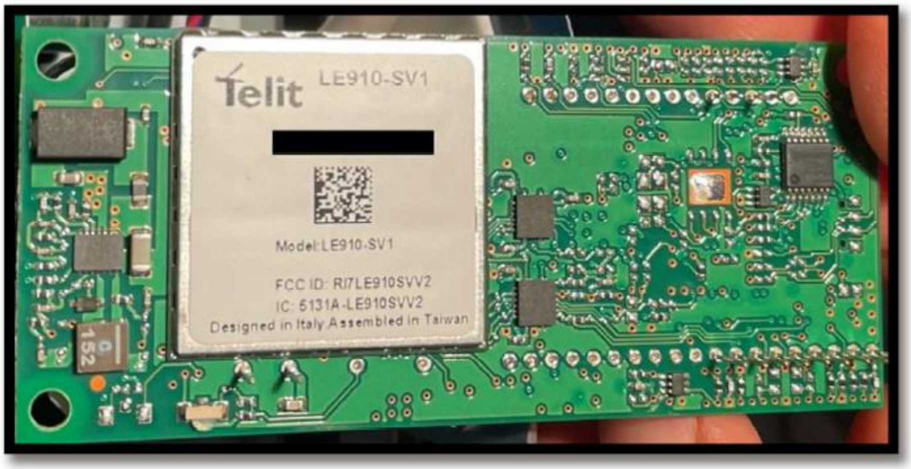
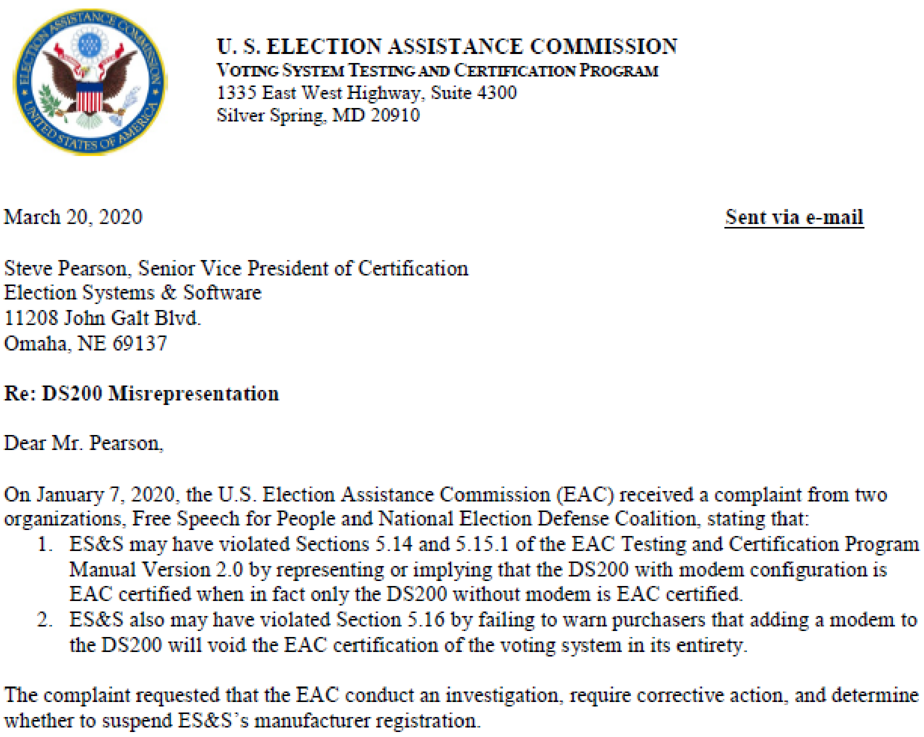


Figure 2 4G Wireless Modem Found Installed On Motherboard of ES&S DS200 Machine

The presence of the modem would be undetected by any election official without any computer engineering expertise or willingness to open up the chassis on the machine. The court exhibit also provided evidence that the modem was used to conduct internet-based communications.

2.3.2.3 Misrepresentation of EAC Certification Status

The Election Assistance Commission (EAC) issued a reprimand to ES&S for promoting claims that their systems which included modems for internet-based communications were fully EAC certified. EAC Testing and Certification standards specifically prohibit internet communications.



U. S. ELECTION ASSISTANCE COMMISSION
VOTING SYSTEM TESTING AND CERTIFICATION PROGRAM
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

March 20, 2020

Sent via e-mail

Steve Pearson, Senior Vice President of Certification
Election Systems & Software
11208 John Galt Blvd.
Omaha, NE 69137

Re: DS200 Misrepresentation

Dear Mr. Pearson,

On January 7, 2020, the U.S. Election Assistance Commission (EAC) received a complaint from two organizations, Free Speech for People and National Election Defense Coalition, stating that:

1. ES&S may have violated Sections 5.14 and 5.15.1 of the EAC Testing and Certification Program Manual Version 2.0 by representing or implying that the DS200 with modem configuration is EAC certified when in fact only the DS200 without modem is EAC certified.
2. ES&S also may have violated Section 5.16 by failing to warn purchasers that adding a modem to the DS200 will void the EAC certification of the voting system in its entirety.

The complaint requested that the EAC conduct an investigation, require corrective action, and determine whether to suspend ES&S's manufacturer registration.

Figure 3 EAC Reprimand of ES&S

2.3.3 Dominion Voting Systems

2.3.3.1 Bluetooth Connections

Dominion ImageCast Central (ICC) workstations in use by Detroit during the 2022 primary election featured terminals compatible with Bluetooth network cards that can be used to provide wireless, tethered connections to the internet.

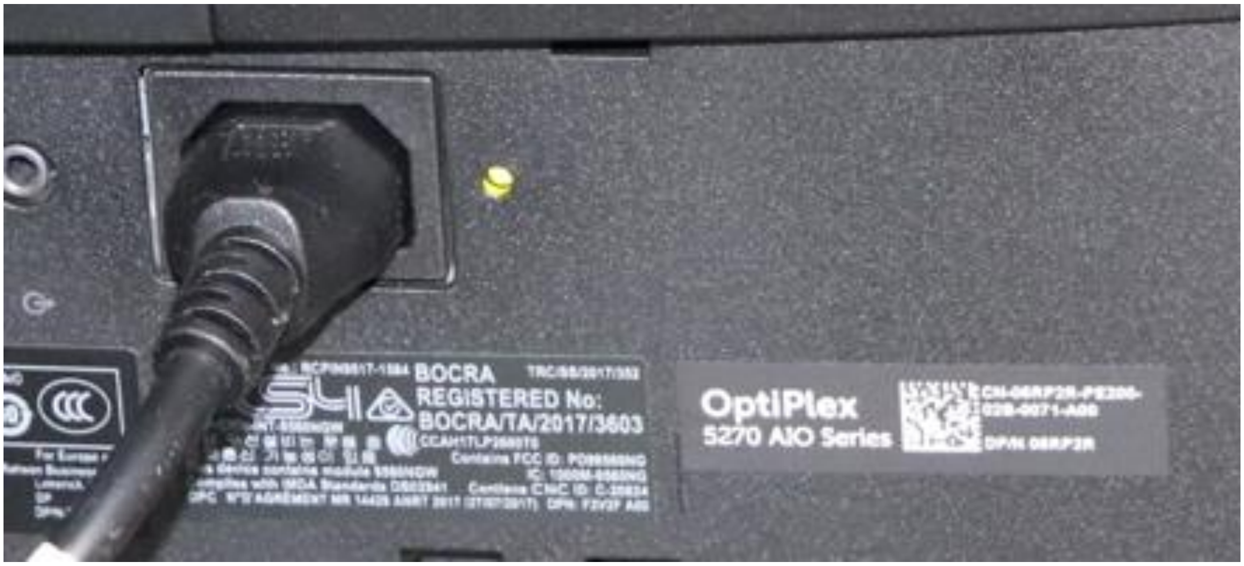


Figure 4 Dominion ICC OptiPlex Workstation Back Panel

Any time one sees an FCC ID on a device label, it indicates that the device is able to support wireless data connections.

Label & Location for 9560NGW this application is only using 1 model 9560NGW

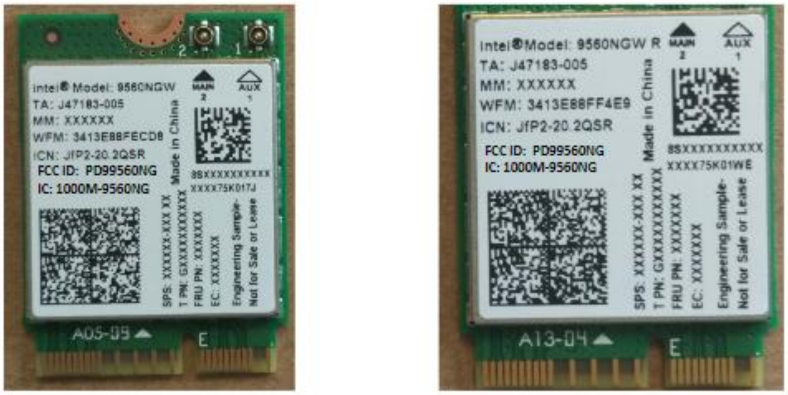


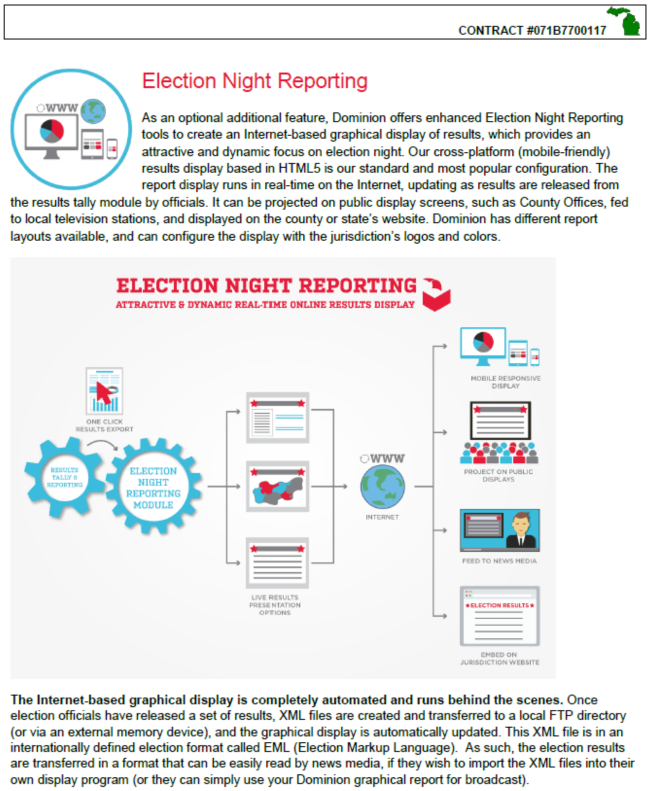
Figure 5 Wireless Cards for Use in OptiPlex Workstations

2.3.3.2 Ethernet Connections

Dominion ICC workstations in use by Detroit during the 2020 general election featured ethernet connections. Affidavits submitted in court cases pertaining to the 2020 election included evidence that these devices were connected to the internet due to the display of the Windows internet connectivity icon on the monitors.

2.3.3.3 Contract

Many local election officials may not have taken the time to review the contracts between their respective states and machine vendors. In states like Michigan, these contracts feature clear evidence that voting systems are designed to connect to the internet.



CONTRACT #071B7700117

Election Night Reporting

As an optional additional feature, Dominion offers enhanced Election Night Reporting tools to create an Internet-based graphical display of results, which provides an attractive and dynamic focus on election night. Our cross-platform (mobile-friendly) results display based in HTML5 is our standard and most popular configuration. The report display runs in real-time on the Internet, updating as results are released from the results tally module by officials. It can be projected on public display screens, such as County Offices, fed to local television stations, and displayed on the county or state's website. Dominion has different report layouts available, and can configure the display with the jurisdiction's logos and colors.

ELECTION NIGHT REPORTING
ATTRACTIVE & DYNAMIC REAL-TIME ONLINE RESULTS DISPLAY
ONE CLICK RESULTS EXPORT
RESULTS TALLY & REPORTING
ELECTION NIGHT REPORTING MODULE
LIVE RESULTS PRESENTATION OPTIONS
WWW
INTERNET
MOBILE RESPONSIVE DISPLAY
PROJECT ON PUBLIC DISPLAYS
FEED TO NEWS MEDIA
ELECTION RESULTS
EMBED ON JURISDICTION WEBSITE

The Internet-based graphical display is completely automated and runs behind the scenes. Once election officials have released a set of results, XML files are created and transferred to a local FTP directory (or via an external memory device), and the graphical display is automatically updated. This XML file is in an internationally defined election format called EML (Election Markup Language). As such, the election results are transferred in a format that can be easily read by news media, if they wish to import the XML files into their own display program (or they can simply use your Dominion graphical report for broadcast).

Figure 6 Page 116 of Contract 071B7700117 Between State of Michigan and Dominion Voting Systems

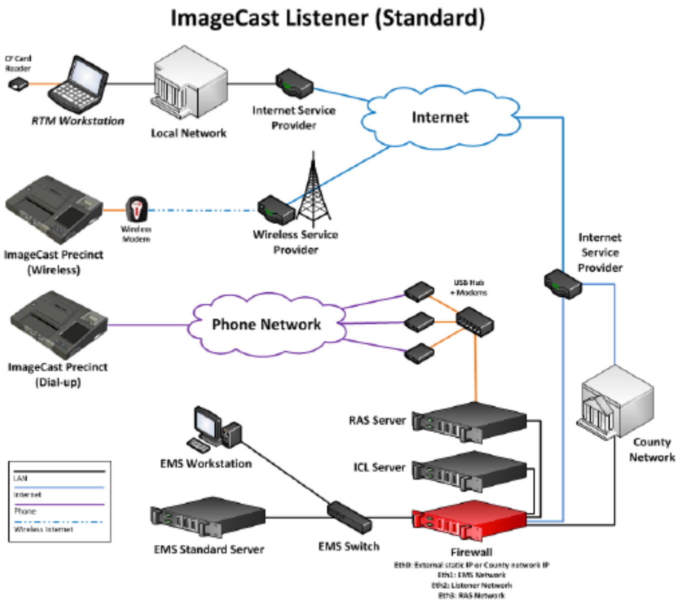


Figure 7 Page 128 of Contract 071B7700117 Between State of Michigan and Dominion Voting Systems

3 Impact

3.1 Violation of Security Standards

EAC specifically prohibits internet connections in their certification standards.

3.2 Shutdown of Election Operations

Systems connected to the internet are vulnerable to power outages, malware, and denial of service attacks which could shutdown election operations or be used to cover-up election malfeasance.

3.3 Election Record Tampering

Internet connections enable remote users to tamper with election records as follows:

- Access and modify voter rolls
- Tamper with ballot definitions
- View or alter vote counts before official release

This undermines the confidentiality and integrity of the entire election process

3.4 Loss of Public Trust

Internet connectivity would also lead to:

- Decreased voter confidence in the election system
- Questions about the validity of results
- Potential legal challenges to election outcomes

Maintaining public trust is critical for democratic elections.

4 Risk Mitigation Strategy

If state law permits the removal of electronic voting systems, election officials should:

- Remove electronic voting systems
- Define and implement hand count procedures
- Maintain local voter rolls on equipment that is not connected to the internet

If state law mandates the use of electronic voting systems, election officials should:

- Ensure transaction logs for all election system components are retained for a period of not less than 22 months after election
- Ensure the preparation of paper copies of key election records prior to and after any digital data transfers of those records
- Use proper key management systems to securely store and manage encryption keys
- Implement strong access controls and authentication for election databases
- Conduct regular security audits to detect vulnerabilities
- Follow NIST guidelines for protecting sensitive election data

In order to conduct a professional audit of elections featuring electronic voting systems it is imperative that there is an audit trail for digital records in much the same way there is an audit trail for paper records.

5 Conclusion

Electronic voting systems are components of our nation’s critical infrastructure. In order to secure the integrity of our elections, we must ensure that we eliminate or mitigate risks to the integrity of our election systems. Internet connectivity introduces significant risks to the integrity of our elections. Election officials need to go beyond security assurances about digital data transfers received during vendor sales pitches or the false sense of security provided by outsourcing election security to a 3rd party such as the Center for Internet Security. As long as we continue to use electronic voting systems, election officials have personal obligations to ensure that the risks inherent with these systems are eliminated or mitigated. Internet connectivity in support of our elections introduces needless risks and therefore should be discouraged at every opportunity.