

Attorney General Dana Nessel
G. Mennen Williams Building, 7th Floor
525 W. Ottawa St.
P.O. Box 30212
Lansing, MI 48909

October 5, 2020

Dear Attorney General Nessel,

We write to you to request your office initiate an inquiry and investigation into Election Systems & Software (ES&S), regarding misrepresentations in its voting system contract with the state of Michigan relevant to the use of the DS200 ballot tabulator with wireless modem.¹

ES&S sold a version of its system to several Michigan localities that is expressly designed to transmit election results from the DS200 ballot tabulator to the election management system via wireless modems. In its contract with Michigan, ES&S characterized this as a connection to “cellular networks,” while simultaneously and repeatedly insisting to both government officials and the public that none of its voting systems *ever* connect to the internet. This false and misleading distinction between “cellular networks” and the internet has been conclusively refuted—ES&S’s systems with modems *are* exposed to the internet.

ES&S should be compelled to remove the wireless modems from its systems at no cost to taxpayers, as required by the contract. If ES&S refuses, your office should consider legal action against ES&S for breach of contract, breach of warranty, and/or fraudulent or reckless misrepresentation. By selling an internet-connected voting system, ES&S has not only misled the voters and local election officials, but also endangered the security of Michigan’s elections.

¹ Free Speech For People is a non-profit, non-partisan public interest legal organization that works to renew our democracy and our United States Constitution for the people. As part of our mission, we are committed to promoting, through legal actions, secure, transparent, trustworthy and accessible voting systems for all voters.

1. Background

a. DS200s with modems are not federally certified

ES&S manufactures the DS200, a precinct-based ballot scanner and vote tabulator. In 2011, ES&S submitted a new voting system, the EVS 5.0.0.0, to the U.S. Election Assistance Commission (EAC) for federal certification. As part of the EVS 5.0.0.0 system, ES&S sought certification of the DS200 in three versions: (1) as a stand-alone precinct scanner, (2) as a precinct scanner with wired modem capability, and (3) as a precinct scanner with wireless network capability. In the third configuration, a wireless modem is present in the polling place tabulation system and used to transmit unofficial election results to the jurisdiction's election management systems. This means both the ballot tabulating machine and the election management system (EMS), a critical component that programs the voting system and aggregates vote totals, connect to the internet.

Unable to meet federal requirements for modems, ES&S withdrew both the wired modem and wireless transmission configurations of the DS200 from their application process in August of 2012.² This version of the EVS 5.0.0.0 system—which does not include either a wired modem or wireless transmission configuration of the DS200—was certified by the EAC to VVSG 1.0 standards on May 13, 2013.³ Several subsequent versions have also been certified, all without modems.

There is widespread consensus among election cybersecurity experts that voting systems with the capability to connect to the internet, through wireless modems or other means, are highly insecure.⁴ In contemplating the security concerns specific to the use of wireless modems in voting systems, the National Institute of Standards and Technology (NIST) wrote:

² Steve Pearson, Vice President, Certification, ES&S, Letter to U.S. Election Assistance Commission Re: EVS 5.0.0.0 Scope Revision (August 13, 2012).

³ ES&S EVS 5.0.0.0 Certificate of Conformance; Alice P. Miller, U.S. Election Assistance Commission, Letter to Steve Pearson, Vice President, Certification, ES&S, Re: Agency Decision—Grant of Certification (May 16, 2013); Wyle Laboratories, Test Report, Report No. T59087.01-01 Rev A (May 1, 2013).

⁴ National Academies of Science, Engineering and Medicine, “Securing the Vote,” 2018. *Available at:* <https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy>

*“If an attacker gains access to the voting system through wireless technology, they may be able to remotely inject malware or modify files within the voting system. This impacts the integrity of the information on the voting system if the malware is able to modify files such as, maliciously tampering with tabulation results or deleting ballot records. The confidentiality of the information on the voting system is impacted if the malware is used to reconfigure the wireless technology to send data to an unauthorized receiver... Exposure to the internet may also enable nation-state attackers to remotely inject malware that maliciously modifies or deletes files within the voting system.”*⁵

According to NIST any device that has this capability can be hacked remotely, including by nation-state actors.⁶

Since initial certification, it is our understanding that ES&S has not submitted a wired modem or wireless configuration of the DS200 for EAC testing or certification. Instead, ES&S offers the DS200 with wireless modem configuration to customers under its never EAC-certified system EVS 5.3.2.0 and other versions.⁷ Though not federally certified, ES&S repeatedly falsely claimed to its customers, in marketing materials and publicly available information, that the DS200 systems with modems were federally certified.⁸

ES&S sold DS200 scanners in seven Michigan counties: Bay County, Emmet County, Grand Traverse County, Kalamazoo County, Macomb County, Mason County, and Roscommon County.⁹ Researchers have found ES&S election management systems for at least four Michigan localities visible on the internet,

⁵ “Draft Recommendations for Requirements for the Voluntary Voting System Guidelines VVSG 2.0,” National Institute of Standards and Technology, January 31, 2020. Available at: <https://collaborate.nist.gov/voting/pub/Voting/VVSG20DraftRequirements/vvsg-2.0-2020-01-31-DRAFT-requirements.pdf>

⁶ *Ibid.*

⁷ Elections System Software, LLC, Exhibit 2, Attachment 1.1 Voting System Hardware, Contract No. 071B7700120 (Mar. 1, 2017), https://www.michigan.gov/documents/sos/071B7700120_ESS_Exh_2_to_Sch_A_Tec_Reg_555360_7.pdf at 1.1.A.17

⁸ Kim Zetter, “Election commission orders top voting machine vendor to correct misleading claims,” *Politico*, August 13, 2020. Available at: <https://www.politico.com/news/2020/08/13/election-voting-machine-misleading-claims-394891>

⁹ See:

<https://verifiedvoting.org/verifier/#mode/search/year/2020/state/26/make/Election%20Systems%20%20Software/model/DS200>

indicating that ES&S delivered this configuration to, at least, these four jurisdictions.¹⁰

b. Contract

In 2017, the Michigan Secretary of State approved three vendor statewide contract proposals, allowing localities to purchase systems under any of the approved contracts.¹¹

The ES&S contract offers a base system and then identifies a proposed modification to the proposed base Michigan voting system, to include the wireless modems. In the contract, ES&S acknowledges that the modification is not EAC certified:

“EVS 5.3.2.0 is a modification of the EVS 5.2.2.0 that allows for the transmission of unofficial election results on election night via landline or wireless modeming from a precinct based DS200 and/or from regional collection sites to election central via the AT&T, Sprint, or Verizon network.”¹²

However, the contract goes on to misstate the difference and omit the fact that the modem modification will make the system internet-connected.

*“**ES&S Footnote:** ES&S confirms that the only functional difference between the Base System (EVS 5.2.2.0.) and the Modified System (EVS 5.3.2.0.) is the addition of modem functionality to allow for electronic transmission of unofficial results.”¹³ (Emphasis added.)*

It is important to understand that in this configuration the connection and exposure to the internet is not limited to the tabulator with the wireless modem. In order to receive the transmitted unofficial results, the election management system (a

¹⁰ Kim Zetter, “Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials,” *Vice*, (Aug. 8, 2019). Available at: https://www.vice.com/en_us/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials

¹¹ See “Voting System Purchase Resources and Instructions for Michigan Election Officials.” Available at: https://www.michigan.gov/sos/0,4670,7-127-1633_11976_78903---,00.html

¹² State of Michigan Enterprise Procurement, Contract No. 071B7700120, Department of Technology, Management, and Budget (Mar. 1, 2017) Exhibit 1 to Schedule A. (page 47). Available at: https://www.michigan.gov/documents/sos/071B7700120_ESS_Contract_555359_7.pdf

¹³ *Ibid.*

critical component of the election system which not only aggregates vote totals but also programs voting machines) must be connected and exposed to the internet for a sustained period of time. This constitutes an additional significant functional difference in that the election management system must be enabled for internet connectivity, have access to the internet, and be actively connected to the internet for sustained periods of time in order to receive the electronic transmission of unofficial results from the modems.

c. ES&S False Claims

Internet connectivity

If Michigan officials did not understand that use of wireless modems directly connect and expose a system to the internet, this can be directly attributed, not just to ES&S's conspicuous omission of this fact, but to potential false claims and misrepresentations made by ES&S in other materials.

Through the contract and in public statements, ES&S represents the wireless modems only as using “cellular networks.” (By contrast, when discussing the transmission and posting of election night reporting systems - which are expected to be transmitted and posted on the public internet - ES&S explicitly acknowledges the transmission will be conducted via the internet.) But much more importantly, ES&S has repeatedly represented to its customers that *none* of its voting systems *ever* connect to the internet. As recently as January 2020, the ES&S website stated:


“Zero. None of our voting tabulators are connected to the Internet.”¹⁴

The screenshot shows the ES&S website with a navigation bar at the top containing 'What We Do', 'Products', 'Security', and 'Resources'. The main heading reads 'Secure. Accountable. Reliable.' Below this, a paragraph states: 'Every time voters head to the polls, they want to know their votes will be accurately counted and protected. At Election Systems & Software, we take extra precautions to ensure our software, hardware and data is well-insulated from harm.' A large orange box contains the text: 'Zero. None of our voting tabulators are connected to the internet.' and '0/1,000,000 Our EAC certified systems are required to complete testing with 0 errors in 1 million test ballots.' To the right of this box is a graphic with the words 'ELECTION SECURITY' in large blue letters, with a blue arrow pointing upwards through the word 'ELECTION'. Below the graphic, a small text block says: 'Learn about the six layers of security that protect ES&S voting systems - from physical security to encryption to verifiable audit trails.'

¹⁴ Internet Archive capture on Jan 10, 2020:
<https://web.archive.org/web/20200110012456/https://www.essvote.com/feature/security/>

Another ES&S webpage titled “Let’s get the facts straight —” stated:

“ES&S voting machines are never connected to the Internet.”¹⁵



[What We Do](#) ▾[Products](#) ▾[Security](#)[Resources](#) ▾

Let’s get the facts straight.

Have America's voting machines been hacked in the past?

While the threats are very real, there's no evidence that any vote in a U.S. election has ever been compromised by a cybersecurity breach. To date, the totality of security measures — such as voting machines never being connected to the internet, tamper-resistant seals, audits, along with more advanced technology found in newer equipment — provides for an environment that would be difficult to compromise. As threats become more sophisticated, so must voting machines and the nation's entire voting infrastructure.

[Click here](#) to download CIS's best practices for securing connected, non-voting election technology.

Can we trust ES&S voting machines?

Voting machines provided by ES&S are certified by the federal Elections Assistance Commission and undergo robust testing for accuracy, reliability, usability and security. ES&S voting machines are never connected to the internet. There is no evidence of a voting machine being compromised by a cybersecurity incident in an election. Voting machines are used and deployed in a decentralized manner across the nation's 10,000 voting jurisdictions. This decentralization greatly diminishes the chance or impact of a large-scale attack. While there is no evidence of any hacking of any voting machine currently in use as it is used in an election, as threats become more sophisticated, so must voting machines and the nation's entire voting infrastructure.

Can voting machines be hacked?

Voting machines have been hacked at conferences and demonstrations, but these environments do not reflect an actual election scenario where additional layers of physical and cyber security are always in place. These measures include, among other steps, voting machines never being connected to the internet, tamper-resistant seals, audits, along with more advanced technology found in newer equipment.

If I have a key that can open an ES&S machine lock, does that mean I can easily get into and hack the machine?

No. Doors and locks are just one of the deterrents to tampering with a voting machine. During an election, there are many security measures beyond doors and locks, including tamper-resistant, serial-numbered seals to ensure security. If a seal is broken, it can't be replaced without detection. We also have multiple layers of encrypted security on the data, including unique encryption keys for every election. This ensures all of our voting machines will only accept USB flash drives programmed for that election and prevents tampering by unauthorized agents.

Why are modems allowed to transmit results?

Where used, cellular modems are only used to transmit unofficial results. Final official results are physically uploaded at election headquarters prior to final certification. The decision to use a modem to transmit unofficial results is made by each jurisdiction. Some jurisdictions choose to use a modem to transmit the unofficial results as quickly as possible, and some choose to receive the unofficial votes once the machines are collected from the polling places.

[Click here](#) to learn more about how election management systems are kept secure in jurisdictions that choose to deliver unofficial election night results by modem.

ES&S has also repeated this misinformation in direct emails to its customers. In an email sent to ES&S customers on the eve of the 2017 DEF CON hackers conference ES&S sent an email to its customers that stated:

¹⁵ Internet Archive capture on Oct. 29, 2019.
<https://web.archive.org/web/20191029124002/https://www.essvote.com/faqs/>

“Can you perform a cyber-attack on something that is not connected to the internet?”

The units that tabulate votes and the computers that contain the software to program those units are NEVER connected to the internet.”¹⁶

ES&S made these claims while selling devices configured specifically to connect to and receive unofficial results over the internet.

Federal Certification

As noted, ES&S’s misstatements regarding its systems with wireless modems extend to misrepresentations regarding federal certification. In January of 2020, Free Speech For People sent a letter to the EAC detailing evidence of false claims and deceptive marketing practices by ES&S designed to misrepresent its voting systems with wireless modems as federally certified. The EAC conducted an investigation and concluded that ES&S misrepresented its systems with modems as federally certified when they were not. The EAC also directed ES&S to contact all its customers that had bought systems with wireless modems and acknowledge that it had falsely claimed its modemed systems had been certified.¹⁷

Though Michigan law does not require EAC certification, the State clearly values it. The Michigan contract explicitly stated:

“A. Federal Testing and Certification Requirements

Contractor’s system shall have been tested and successfully completed all certification steps required by the U.S. Election Assistance Commission (EAC) before the system will be approved for implementation in Michigan.”¹⁸

In short, ES&S appears to have misled Michigan officials to believe that its modemed systems use “cellular networks,” not the internet, because ES&S voting systems “never” connect to the internet. ES&S also advertised its systems with

¹⁶ See attachment A.

¹⁷ See: Zetter, note 8.

¹⁸ State of Michigan Enterprise Procurement, Contract No. 071B7700120, Department of Technology, Management, and Budget (Mar. 1, 2017) page 24.

https://www.michigan.gov/documents/sos/071B7700120_ESS_Contract_555359_7.pdf
At 1.5.A

modems as federally certified when they are not, and ES&S claimed that the only functional difference from its federally certified system is the transmission of election results, without acknowledging that both the voting tabulator and critical election management system must be connected to the internet.

2. Grounds to compel removal of modems

In August of 2019, a news report disclosed that researchers had identified ES&S EMSs on the internet in Michigan, meaning that they could clearly identify the IP addresses of ES&S EMSs on the internet in the state. This means the EMSs were connected to the internet and visible to the ethical researchers as well as malicious actors. The researchers reported that even after notifying the national Elections Infrastructure and Information Sharing and Analysis Center (EI-ISAC)—a 24-hour watch center funded by the Department of Homeland Security—of their discovery, systems in Kalamazoo and Roscommon remained online. Another Michigan system was also online, but researchers were unable to pinpoint the jurisdiction in which the IP address is located.¹⁹

The state should compel ES&S to remove the modems at no cost to the state or localities. Michigan Secretary of State Jocelyn Benson later commented that if her cybersecurity election committee recommends the modems be taken out, “we’ll take them out.”²⁰ Removing these modems may prove costly. However, the contract obligates ES&S to cure any “defects or malfunctions” in the system, as provided in Section 1.6 of the Contract’s statement of work:

“Contractor shall promptly notify the State and any Authorized User of any defects or malfunctions in the Deliverable, associated System Software or Documentation of which it learns from any source, correct any such defects or malfunctions or provide a workaround until corrected within five (5) Business Days of knowledge of such defect or malfunction and provide the

¹⁹ See: Zetter, note 10.

²⁰Kartikay Mehrotra, “America Won’t Give Up Its Hackable Wireless Voting Machines (1),” Bloomberg Law, (Jan. 3, 2020), <https://news.bloomberglaw.com/privacy-and-data-security/america-wont-give-up-its-hackable-wireless-voting-machines>.

State or Authorized User with corrections of same, at no additional cost to the State or Authorized User.”²¹

The systems with internet connectivity should constitute a “defect,” as they do not conform to the contract’s terms. Consequently, upon demand, ES&S must, within five business days, correct this defect “at no additional cost” to the state or localities.

If ES&S does not agree to correct this defect within five business days after your demand, your office should consider judicial action. If it turns out that, by including internet connectivity in its modems, ES&S either breached an express warranty, engaged in misrepresentation, or else breached the contract, the state may be able to compel ES&S to remove the modems at no cost.

By including the EVS 5.3.2.0 in its product options for Michigan counties, ES&S may have breached an express warranty. Specifically, by warranting that its voting system conforms to the specifications set forth in the contract, ES&S may have also warranted that its voting systems do *not* connect to the internet.²² Specifically, as noted above, in the contract ES&S “confirm[ed] that the only functional difference between the Base System (EVS 5.2.2.0.) and the Modified System (EVS 5.3.2.0.) is the addition of modem functionality to allow for electronic transmission of unofficial results.”²³ And while today’s cellular modems do connect to the internet, the fact that ES&S expressly warranted that the “only” functional difference was connecting to cellular data networks means that their connection to the internet is contrary to this warranty. Further, ES&S neatly omits the fact that the EMS must be enabled for internet connectivity, requires access to an internet connection and must have a live internet connection to receive the transmission.

²¹ State of Michigan Enterprise Procurement, Contract No. 071B7700120, Department of Technology, Management, and Budget (Mar. 1, 2017) at 1.6.A.2 (p.

26).https://www.michigan.gov/documents/sos/071B7700120_ESS_Contract_555359_7.pdf

²² Elections System Software, LLC, Exhibit 2, Attachment 1.1 Voting System Hardware, Contract No. 071B7700120 (Mar. 1, 2017),

https://www.michigan.gov/documents/sos/071B7700120_ESS_Exh_2_to_Sch_A_Tec_Reg_555360_7.pdf at 1.2.A.3.

²³ See: note 18 at Exhibit 1 to Schedule A (C).

Consequently, EVS 5.3.2.0 has an important functional difference (internet connectivity) with EVS 5.2.2.0 that was not disclosed—a violation of ES&S’s express representation that “the only functional difference” was functionality enabling connection via landline or specified cellular data networks. Moreover, this lack of conformity may also represent a general breach of contract. If so, the state must give the vendor at least 30 days to cure such a breach or else the State may terminate the contract for cause, in whole or in part.²⁴

3. Conclusion

As the country approaches to the 2020 election—the first presidential election since 2016 when Russian hackers attempted to infiltrate numerous voting systems across the United States—it is critical, now more than ever, that states across the nation secure the safety of our elections. This includes ensuring that voting systems cannot be hacked remotely by sophisticated hackers because those systems connect to the internet. The Michigan Attorney General should act now to investigate Michigan’s contract with ES&S in order to compel the removal of wireless, internet-connecting modems in DS200s across the state.

Please do not hesitate to reach out to us if you have any questions or if we can be of any assistance. We stand ready to assist you and your colleagues in any way we can.

Sincerely,

Susan Greenhalgh
Senior Advisor on Election Security
susan@freespeechforpeople.org

Ron Fein
Legal Director
RFein@freespeechforpeople.org

cc. The Honorable Jocelyn Benson
Michigan Department of State
Bureau of Elections
PO Box 20126
Lansing, MI 48901-0726

²⁴ State of Michigan Enterprise Procurement, Contract No. 071B7700120, Department of Technology, Management, and Budget (Mar. 1, 2017) at pg.14.
https://www.michigan.gov/documents/sos/071B7700120_ESS_Contract_555359_7.pdf