pennsylvania
DEPARTMENT OF STATE

Report Concerning the Reexamination of Dominion Democracy Suite 5.5-A

SECRETARY OF THE COMMONWEALTH
PENNSYLVANIA

Issued By:

Al Schmidt

Secretary of the Commonwealth

August 11, 2025

Contents

I. INTRODUCTION 4

II. THE DEMOCRACY SUITE 5.5-A SYSTEM 5

Election Management System (EMS) 5

EMS Election Event Designer (EED) 5

EMS Audio Studio (AS) 5

EMS Application Server 5

EMS Results, Tally, and Reporting (RTR) 5

EMS File System Service (FSS) 5

EMS Data Center Manager (DCM) 6

EMS Election Data Translator (EDT) 6

EMS Adjudication (ADJ) 6

EMS ImageCast Voter Activation (ICVA) 6

ImageCast X Ballot Marking Device (BMD) 6

ImageCast Central (ICC) Central Count Tabulator 6

ImageCast Precinct (ICP) Precinct Tabulator 6

Manufacturer Software/Firmware 7

Commercially Available Over the Counter Software and Firmware 7

III. REEXAMINATION APPROACH 8

A. Approach Summary 8

B. Scope 8

C. Limitations 8

D. Test Materials 8

IV. REEXAMINATION RESULTS AND DISCUSSION 9

Allegation #1 – Cryptographic Keys are Stored in Plaintext 9

Allegation #2 – Results May be Tampered with Prior to Loading 9

Allegation #3 – Tabulators can be Reconfigured 9

Allegation #4 – Votes and Tallies are Directly Modifiable in SSMS 9

Allegation #5 – Windows Login can be Bypassed 9

Allegation #6 – SSMS is Accessible via Windows Authentication 9

Allegation #7 – Password Reuse 10

Allegation #8 – iButton HMAC Compromise Enables Altering Election Results 10

Allegation #9 – X.509 Compromise Enables Data Interception/Altering 10
Allegation #10 – Systems are Compromised by Sleeper Malware... 10
V. CONCLUSION.. 11
Appendix A – Petition Copy 12
Appendix B – EAC Certification Scope 13

I. INTRODUCTION

Article XI-A of the Pennsylvania Election Code, 25 P.S. § 3031.1 *et seq*., authorizes the use of electronic voting systems. Section 1105-A of the Pennsylvania Election Code, 25 P.S. § 3031.5(a), allows any ten or more qualified electors of Pennsylvania to request a reexamination of an electronic voting system certified by the Secretary of the Commonwealth ("Secretary"). On November 1, 2024, the Secretary received a Petition to Reexamine Democracy Suite 5.5-A (the "Petition"). A copy of that Petition is attached hereto as Appendix A.

The Democracy Suite 5.5-A electronic voting system was initially examined and certified to both federal and state voting system standards by the Election Assistance Commission ("EAC") on January 30, 2019, and by the Secretary on January 17, 2019, respectively.

The Petition sets forth allegations as to why the Secretary should de-certify the Democracy Suite 5.5-A electronic voting system. After a thorough and considered review of the Petition, the Secretary, in consultation with the Department of State staff, entered into an agreement with SLI Compliance ("SLI"), a federally accredited voting systems test laboratory, to conduct a focused reexamination of the Democracy Suite 5.5-A electronic voting system with respect to the allegations set forth in the Petition.

The off-site reexamination was conducted at the laboratory of SLI Compliance in Wheat Ridge, Colorado. The examiners then provided findings from the examination, and the results and conclusions have been included in Sections IV and VI of this report.

II. THE DEMOCRACY SUITE 5.5-A SYSTEM

Democracy Suite 5.5-A components considered for use in Pennsylvania1 provide a paper-based voting system with end-to-end election support, from defining an election to generating final reports. The system is comprised of both precinct and central count tabulators, and BMDs as the ADA component. The system components include: the Election Management System (EMS), the ImageCast Central (ICC) - utilizing two Commercial Off the Shelf (COTS) scanners, the ImageCast Precinct (ICP) optical scanner and the ImageCast X (ICX) (Prime and Classic) ballot marking devices.

The following is a description of the Democracy Suite 5.5-A components summarized from Section 2.0 (System Overview) of the Test Report for Examination of Democracy Suite 5.5-A, prepared by the Functional Examiner and documentation submitted by Dominion as part of the Technical Data Package (TDP).

Election Management System (EMS)

The Dominion Democracy Suite 5.5-A EMS supports elections on the ICX Prime, ICX Classic, ICP and ICC systems. The EMS set of applications are responsible for all pre and post-voting groups of activities in the process of defining and managing elections. EMS software platform consists of end-user (client) and back-end (server) applications. The EMS platform consists of the following major components.

EMS Election Event Designer (EED)

Supports pre-voting activities including election definition together with ballot styling capabilities.

EMS Audio Studio (AS)

End-user helper application used to record audio files for a given election project utilized during the pre-voting phase of the election cycle.

EMS Application Server

Server-side application responsible for executing long running processes, such as rendering ballots, generating audio files and election files, etc.

EMS Results, Tally, and Reporting (RTR)

Integrates election results acquisition, validation, tabulation, reporting, and publishing capabilities and represents a main postvoting phase end-user application

EMS File System Service (FSS)

Stand-alone service that runs on client machines, enabling access to low level operating system API for partitioning CF cards, reading raw partition on ICP CF card, etc.

EMS Data Center Manager (DCM)

End-user application used to export election data from election project and import election data into election project.

EMS Election Data Translator (EDT)

End-user application used to export election data from election project and import election data into election project.

EMS Adjudication (ADJ)

Server and client components responsible for adjudication, including reporting and generation of adjudicated 6 result files from ImageCast Central tabulators and adjudication of write-in selections from ImageCast Precinct and Image Cast Central tabulators

EMS ImageCast Voter Activation (ICVA)

Installed on a workstation or laptop at the polling place, that allows the poll workers to program smart cards for voters. The smart cards are used to activate voting sessions on ImageCast X

ImageCast X Ballot Marking Device (BMD)

The ICX ballot marking platform is used for creation of paper cast vote records. These ballots can be scanned, reviewed, cast and tabulated at the polling location on an ICP or later scanned and tabulated by the ICC at a central location. The ICX consists of two models, ICX Prime and ICX Classic

ImageCast Central (ICC) Central Count Tabulator

The ICC is a high-speed, central ballot scan tabulator based on Commercial off the Shelf (COTS) hardware, coupled with the custom-made ballot processing application software. It is used for high speed scanning and counting of paper ballots.

ImageCast Precinct (ICP) Precinct Tabulator

The ICP is a hybrid precinct optical scan ballot counter designed to provide ballot scanning, ballot review and tabulation at a polling place.

Manufacturer Software/Firmware

The Dominion Democracy Suite 5.5-A voting system consists of the following software and firmware components:

Application	Version
EMS Election Event Designer (EED)	5.5.12.1
EMS Results Tally and Reporting (RTR)	5.5.12.1
EMS Application Server	5.5.12.1
EMS File System Service (FSS)	5.5.12.1
EMS Audio Studio (AS)	5.5.12.1
EMS Data Center Manager (DCM)	5.5.12.1
EMS Election Data Translator (EDT)	5.5.12.1
ImageCast Voter Activation (ICVA)	5.5.12.1
EMS Adjudication	5.5.8.1
EMS Adjudication Service	5.5.8.1
Smart Card Helper Service	5.5.12.1
ImageCast Precinct	5.5.3.0002
ImageCast Central	5.5.3.0002
ImageCast X	5.5.10.30

Commercially Available Over the Counter Software and Firmware

Additional COTS software and firmware included in the system has been defined as part of the EAC system certification scope that will be added to this report as Attachment B.

III. REEXAMINATION APPROACH

A. Approach Summary

The reexamination focused on the alleged violations of the Pennsylvania Election Code and the Pennsylvania Voting System Security Standard as outlined in the Petition. The Examiner evaluated the Petition and relevant system documentation to develop test protocols for the reexamination with regard to the specific allegations. All hardware necessary to perform the reexamination was supplied by Dominion Voting Systems. This reexamination was performed in-house at SLI Compliance, with installation and configuration of EAC certified Democracy Suite 5.5-A performed by Dominion representatives and observed by SLI Compliance. Hash validation performed by SLI Compliance verified that the installed system matched the EAC certified system.

B. Scope

This reexamination scope was limited to Democracy Suite 5.5-A voting system equipment certified for use in the Commonwealth of Pennsylvania.

The SLI Compliance security team conducted the reexamination against the following Democracy Suite 5.5-A certified voting system equipment. The ImageCast Evolution (ICE) is referenced by the Petition, but not part of the system as certified for use and was thus not included in the reexamination.

- Election Management System (EMS) Standalone Server – "EMS Server"
- Election Management System (EMS) Client Workstation – "EMS Client"
- ImageCast Central (ICC) Client Workstation – "ICC"
- Canon ImageFormula DR-G2140 scanner – "ICC Scanner"
    - ImageCast Precinct (ICP) Tabulator – "ICP"
- ImageCast X (ICX) Ballot Marking Device (BMD) – "ICX"
- ImageCast Voter Activation (ICVA) for ICX – "ICVA"

C. Limitations

The testing and analysis performed during this reexamination was limited to evaluating claims made in the Petition regarding the security of the voting system with respect to the Pennsylvania Election Code and the PA Voting System Security Standard.

D. Test Materials

- Test support materials utilized during the examination included:
- Removable storage media for all equipment (USB, CompactFlash)
- iButtons
- Ballot paper
- Democracy Suite 5.5-A sample general election: "PA Cert General 2018"

IV. REEXAMINATION RESULTS AND DISCUSSION

The Examiner thoroughly evaluated the Petition and derived 10 main allegations to be investigated as part the focal points of the reexamination. Listed below is a summary of the allegations and the results of the Examiner's findings regarding each.

Allegation #1 – Cryptographic Keys are Stored in Plaintext

Petition alleged that *"The master cryptographic key … was found to be stored in plain text within the Dominion database";* Examiner's investigation noted no violation of the Pennsylvania Election Code or Pennsylvania Voting System Standard.

Allegation #2 – Results May be Tampered with Prior to Loading

Petition alleged that *"This critical security failure allows a malicious actor to easily alter election results before they are even loaded into the EMS Server" and "… decrypting these [results] files, altering the vote counts or other data, and then re-encrypting … [would be] accepted by the EMS.";* Examiner's investigation noted no violation of the Pennsylvania Election Code or Pennsylvania Voting System Standard.

Allegation #3 – Tabulators can be Reconfigured

Petition alleged that *"A malicious actor could decrypt, alter, and re-encrypt files used to program tabulators. This could change how the tabulators record, count, or report votes…";* Examiner's investigation noted no violation of the Pennsylvania Election Code or Pennsylvania Voting System Standard.

Allegation #4 – Votes and Tallies are Directly Modifiable in SSMS

Petition alleged that *"… Microsoft SQL Server and SSMS allow for easy manipulation of votes and vote tallies";* Examiner's investigation noted no violation of the Pennsylvania Election Code or Pennsylvania Voting System Standard.

Allegation #5 – Windows Login can be Bypassed

Petition alleged that the Windows Login for Democracy Suite 5.5-A Servers can be bypassed*;* Examiner's investigation noted no violation of the Pennsylvania Election Code or Pennsylvania Voting System Standard.

Allegation #6 – SSMS is Accessible via Windows Authentication

Petition alleged that *"Once intruders bypass the Windows login, they gain unrestricted access to the Election Database. This is primarily due to the SQL Server's reliance on flawed Windows Authentication, which does not require additional passwords for database access.";* Examiner's investigation noted no violation of the Pennsylvania Election Code or Pennsylvania Voting System Standard.

Allegation #7 – Password Reuse

Petition alleged that *"… the same password used since 2008 was publicly disclosed … The discovery of the password hash online means that it is more than likely that a person has had access to the database …";* Examiner's investigation noted no violation of the Pennsylvania Election Code or Pennsylvania Voting System Standard. Documentation for Democracy Suite 5.5-A as well Pennsylvania's Certification Report for the voting system both state that account passwords must be changed following installation and configuration. This procedure is expected to be followed by the jurisdiction.

Allegation #8 – iButton HMAC Compromise Enables Altering Election Results

Petition alleged that *"If the process of programming these iButtons is compromised, unauthorized individuals can alter an election result.";* Examiner's investigation noted no violation of the Pennsylvania Election Code or Pennsylvania Voting System Standard.

Allegation #9 – X.509 Compromise Enables Data Interception/Altering

Petition alleged that *"In summary, using X.509 data in election systems to encrypt network traffic is critical for ensuring the voting process remains secure and trustworthy. It safeguards against threats like eavesdropping, data tampering, and unauthorized access…";* Examiner's investigation noted no violation of the Pennsylvania Election Code or Pennsylvania Voting System Standard.

Allegation #10 – Systems are Compromised by Sleeper Malware

Petition alleged that *"Indeed, it is highly likely that many, if not most, election systems are currently compromised by either sleeper malware installed on the systems or are open to malicious actors…";* Examiner's investigation noted no violation of the Pennsylvania Election Code or Pennsylvania Voting System Standard.

V. CONCLUSION

As a result of the reexamination, and after consultation with the Department's staff, counsel, and the Examiners, the Secretary of the Commonwealth concludes that Democracy Suite 5.5-A electronic voting system previously certified can be safely used by voters at elections, as provided in the Pennsylvania Election Code, and meets all of the requirements set forth in the Election Code, **<u>provided the voting system is implemented under the conditions listed in Section IV of the initial certification report released on Jan 17th, 2019 and the conditions listed in Section V of this report.</u>** Accordingly, the Secretary maintains the certification of Democracy Suite 5.5-A for use this Commonwealth.

Appendix A – Petition Copy

5.5A Request for
Reexamination.pdf

Dated: October 25, 2024

Honorable Al Schmidt
Secretary of the Commonwealth
Pennsylvania Department of State
401 North Street, Room 302
Harrisburg PA 17120

Dear Secretary Schmidt:

Pursuant to 25 Pa.Stat. § 3031.5, on behalf of the undersigned electors of the Commonwealth of Pennsylvania, we hereby request re-examination of the Dominion Democracy Suite 5.5-A. See Banfield v. Aichele, 51 A.3d 300, 314 (Pa. Cmwlth. 2012) ("The Secretary's duty to re-examine the machines upon proper request is mandatory."). We enclose at least ten (10) certifications of duly registered electors in the Commonwealth of Pennsylvania who seek this re-examination. We have enclosed a check for $450.00 payable to the Treasurer of the Commonwealth of Pennsylvania.

We have attached a statement explaining deficiencies that the undersigned electors believe exist in the Dominion Democracy Suite 5.5-A. We request that you give these issues specific attention during re-examination. Based on these deficiencies, we respectfully request that the Secretary of the Commonwealth re-examine the Dominion Democracy Suite 5.5-A electronic voting machine and issue a report relating to the integrity or vulnerability of the system. We request that this re-examination be conducted expeditiously because several counties in the Commonwealth have chosen the Dominion Democracy Suite 5.5-A, and the upcoming general election could possibly be one of the most monumental elections in American history.

Respectfully submitted,

Request for Re-Examination of the Dominion Democracy Suite 5.5-A

1. I, David H Zimmerman, being a duly qualified and registered elector in the precinct of 4301, located in Lancaster County, Pennsylvania, hereby request that the Secretary of the Commonwealth of Pennsylvania conduct a re-examination of the Dominion Democracy Suite 5.5-A, and request that the re-examination be completed on an expedited basis.

David H Zimmerman
Name: Print

Name: Signature

Oct. 22, 2024
Date

2. I, James Walsh, being a duly qualified and registered elector in the precinct of Ross Twp, located in Luzerne County, Pennsylvania, hereby request that the Secretary of the Commonwealth of Pennsylvania conduct a re-examination of the Dominion Democracy Suite 5.5-A, and request that the re-examination be completed on an expedited basis.

James Walsh
Name: Print

Name: Signature

10-21-24
Date

3. I, Kathy L. Rapp, being a duly qualified and registered elector in the precinct of Conewango II, located in Warren County, Pennsylvania, hereby request that the Secretary of the Commonwealth of Pennsylvania conduct a re-examination of the Dominion Democracy Suite 5.5-A, and request that the re-examination be completed on an expedited basis.

Kathy L. Rapp
Name: Print

Kathy L. Rapp
Name: Signature

10-26-2024
Date

4. I, Matthew J. Contreras, being a duly qualified and registered elector in the precinct of Milford Township, located in Pike County, Pennsylvania, hereby request that the Secretary of the Commonwealth of Pennsylvania conduct a re-examination of the Dominion Democracy Suite 5.5-A, and request that the re-examination be completed on an expedited basis.

Matthew J. Contreras
Name: Print

Matthew J. Contreras
Name: Signature

10/23/2024
Date

5. I, Seerán Eve Mizii, being a duly qualified and registered elector in the precinct of #3302 Swartzville, located in Lancaster County, Pennsylvania, hereby request that the Secretary of the Commonwealth of Pennsylvania conduct a re-examination of the Dominion Democracy Suite 5.5-A, and request that the re-examination be completed on an expedited basis.

Seerán Eve Mizii
Name: Print

Seeran Eve Mizii
Name: Signature

10/24/2024
Date

6. I, Diane Houser, being a duly qualified and registered elector in the precinct of 659 Úwchlan 7, located in Chester County, Pennsylvania, hereby request that the Secretary of the Commonwealth of Pennsylvania conduct a re-examination of the Dominion Democracy Suite 5.5-A, and request that the re-examination be completed on an expedited basis.

Diane Houser
Name: Print

Diane Houser
Name: Signature

October 25, 2024
Date

7. I, Charles Faltenavich, being a duly qualified and registered elector in the precinct of Hopewell 30-02 located in Beaver County, Pennsylvania, hereby request that the Secretary of the Commonwealth of Pennsylvania conduct a re-examination of the Dominion Democracy Suite 5.5-A, and request that the re-examination be completed on an expedited basis.

Charles Faltenavich
Name: Print

Charls Faltavich
Name: Signature

10/23/2024
Date

8. I, WILLIAM L DOUGHERTY, being a duly qualified and registered elector in the precinct of 28 SOUTH ANNVILLE TWP., located in LEBANON County, Pennsylvania, hereby request that the Secretary of the Commonwealth of Pennsylvania conduct a re-examination of the Dominion Democracy Suite 5.5-A, and request that the re-examination be completed on an expedited basis.

WILLIAM L DOUGHERTY
Name: Print

William L Day
Name: Signature

10/24/24
Date

9. I, DAN N. ALTMAN being a duly qualified and registered elector in the precinct of BOROUGH OF FOX CHAPEL DIST. 2, located in ALLEGHENY County, Pennsylvania, hereby request that the Secretary of the Commonwealth of Pennsylvania conduct a re-examination of the Dominion Democracy Suite 5.5-A, and request that the re-examination be completed on an expedited basis.

DAN N. ALTMAN
Name: Print

Dan N. Altman
Name: Signature

10/29/24
Date

10. I, FRANK SCAVO, being a duly qualified and registered elector in the precinct of OLD FORGE 3-0, located in LACKAWANNA County, Pennsylvania, hereby request that the Secretary of the Commonwealth of Pennsylvania conduct a re-examination of the Dominion Democracy Suite 5.5-A, and request that the re-examination be completed on an expedited basis.

FRANK SCAVO		10-29-2024
Name: Print	Name: Signature	Date

Attachment: Deficiency in the Dominion Democracy Suite 5.5-A

We seek re-examination of the Dominion Democracy Suite 5.5-A voting machine because we believe that the manufacturer, Dominion Voting Systems ("Dominion"), has stored master cryptographic keys, which are used to encrypt/decrypt system passwords and election data, in an unprotected state and in plain text on an election database table within Dominion's voting systems. Ultimately, this vulnerability, along with others, may result in multiple election security breaches and compromise the basic integrity of the elections in which this voting system is used.

I. Background

According to the 2015 Federal Voluntary Voting System Guidelines ("VVSG"), Volume 1, Version 1.1, which are standards adopted by the United States Election Assistance Commission ("EAC") for the certification of voting systems, the term "encryption" is defined at Appendix A, in the "Glossary" section, as the "[p]rocess of obscuring information by changing plain text into ciphertext for the purpose of security or privacy." Further, the term "cryptographic key," is defined as the "[v]alue used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification." Moreover, at section 7.7.3 of the VVSG, titled "Protecting Transmitted Data," the EAC states, in pertinent part:

> The transmitted data, especially via wireless communications, needs to be protected to ensure confidentiality and integrity. Examples of election information that needs to be protected include: ballot definitions, voting device counts, precinct counts, opening of poll signal, and closing of poll signal. . . . Thus, encryption is required to protect the privacy and confidentiality of the voting information.
>
> ***
>
> a. All information transmitted via wireless communications **shall** be encrypted and authenticated . . .
> i. Cryptography used for encryption and authentication **shall** use NIST approved algorithms with security strength of at least 112 bits. Message Authentication Code (MAC) keys shall have a security strength of at least 112 bits.
> ii. The cryptographic modules used **shall** comply with FIPS 140-2, Security Requirements for Cryptographic Modules.
> b. The capability to transmit non-encrypted and non-authenticated information via wireless communications **shall** not exist.

(emphasis in original).

In attachment E to the Directive for Electronic Voting Systems, titled, "PA Voting System Security Standard," the Pennsylvania Department of State "outlines the security testing standard . . . for use in the Pennsylvania state certification examination," in order to ensure compliance with the Pennsylvania Election Code. At Section 4.3, "Security Software," under the heading, "Encryption," certain validations must be met:

> **4.3 Software Security**
>
> ***

Encryption

1. Confirm confidentiality of the data is maintained during transmission of sensitive data through the use of encryption.
2. Confirm any data at rest cannot be modified by unauthorized actors. The tests must evaluate access control, encryption, physical security, and chain of custody, and ensure that layers of security exist to prevent unauthorized access to and/or modification of data.
3. Confirm the system cannot transmit non-encrypted and non-authenticated data. The test must include any network transmissions and any transmissions via physical media. The testing team must evaluate the entire data life cycle starting with election preparation until canvassing.
4. Confirm the system uses encryption and cryptographic standards set by recognized standard setting body (NIST, EAC) and industry wide best practices.

On January 17, 2019, the Secretary of the Commonwealth certified the Dominion Democracy Suite 5.5-A. In the upcoming general election, the Dominion Democracy Suite 5.5-A will be used in at least eleven (11) counties—Armstrong, Carbon, Clarion, Crawford, Erie, Fayette, Fulton, Luzerne, Montgomery, Warren, and York. However, beginning in 2020, it appears that Dominion has enabled unauthorized control over and access to its electronic voting systems, by storing its cryptographic keys in an unsecure manner. If someone has access to decryption keys, that person can directly access the voting system and use the cryptographic keys, along with other tools, to alter election results before or after loading election results into the Election Management System ("EMS") without likely detection. In other words, it appears that Dominion, or any actor who possesses the requisite knowledge, can gain total access and control over elections in the counties using Dominion's systems and modify, fabricate, and transmit fake election results.

II. Election Management System Security Analysis

Recently, cyber security experts completed a security analysis of the EMS used in current electoral processes, with a particular focus on the findings from Antrim County, Michigan, four counties in Georgia, Fulton County, Pennsylvania, and subsequent revelations from the Maricopa 2020 Senate Audit. See attached affidavits of Clay U. Parikh and Benjamin Cotton. The analysis was rooted in a detailed examination of system vulnerabilities, particularly in cryptography and secret storage, as highlighted in the April 4th, 2021 report on Antrim County's EMS.

As a major component to this analysis, the cyber security experts made an alarming discovery and finding regarding the storage and handling of the master cryptographic key with respect to Dominion voting machines. The master cryptographic key, fundamental to the encryption of all voting results and configuration data from tabulators and the encryption of tabulator passwords, was found to be stored in plain text within the Dominion database. This critical security failure allows a malicious actor to easily alter election results before they are even loaded into the EMS Server. With this capability, a malicious actor can re-configure tabulators to create fraudulent votes or even an alternate election without likely detection.

Building upon these initial findings, the cyber security experts performed further analysis of the Dominion EMS' database and tabulator storage media backups, which were obtained during the

Maricopa 2020 Senate Audit, and bring to light the broader implications and the depth of the security failures present. The following sections will discuss the security failures, their impact on election integrity, and the ease with which they could be exploited.

III. The Original Finding Regarding Cryptographic Keys in Plain Text

In the April 4th, 2021, report – *Antrim County, MI – Election Management System Application Security Analysis* – at section 6.3, "Cryptography & Secret Storage," the author noted:

> The master cryptographic key utilized to encrypt all voting results and configuration from the tabulators is stored in plain text in a table within the database for this election. With this key and knowledge about the file formats utilized, it would be possible to alter election results prior to those result files being loaded into the EMS Server or to alter configurations for the tabulators to make them behave in a certain way.

Regarding the vulnerability that accompanies open and unauthorized access to cryptographic keys in voting machines, one cyber security expert stated: "Simply put, this is like a bank having the most secure vault in the world, touting how secure it is to the public and then taping the combination in large font type on the wall next to the vault door." Obviously, there is no legitimate reason to store the encryption keys in an unprotected state where numerous, unauthorized individuals could potentially alter the outcome of an election.

IV. Who has the Cryptographic Keys to Our Election

In sum, those who have access to EMS have access to cryptographic keys, including third-party vendors, County contractors, and Dominion Personnel who have full access to the system.

In numerous County elections, the design and setup of elections, including ballot layout and configuration of tabulator files, are outsourced to third-party vendors. These vendors utilize specialized election software for this purpose. A critical part of this process is the vendor's creation of security keys. After delivering the configuration files to the Counties, these vendors retain the keys, allowing the vendor to modify how tabulators interpret and report election results without likely detection.

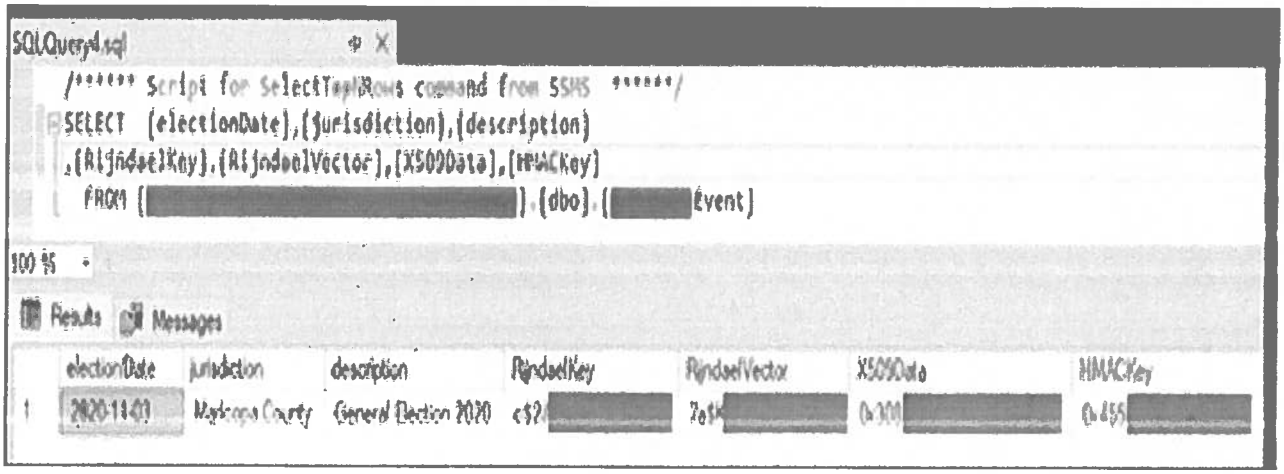
The security protocol within the EMS, specifically in its use of Microsoft SQL Server and SQL Server Management Studio ("SSMS"), allows for easy manipulation of votes and vote tallies. Once intruders bypass the Windows login, they gain unrestricted access to the Election Database. This is primarily due to the SQL Server's reliance on flawed Windows Authentication, which does not require additional passwords for database access.

Upon gaining access, the intruder or unauthorized user can easily view the security keys associated with election files and reports and the passwords for the EMS' user accounts. Notably, no meaningful security measures protect the administrator passwords from loading election results.

V. Instances where Cryptographic Keys and Administrator Passwords became Accessible

One example where cryptograph keys became readily accessible is located in the "Election Event" table in the "20201103 General-2020-09-21-11-26-56" database from the Maricopa 2020 General election. The table shows four different security keys used to encrypt election files to and from the tabulators, authenticate administrators, encrypt tabulator passcodes, and securely send data from one machine to the other.

Below is a screen shot of a table located in Dominion's own election project databases, containing four encryption keys: the Rijndael Key;[1] the Rijndael Vector;[2] the X509 Certificate; and the Hash-Based Message Authentication Code ("HMAC"):[3]



```
/****** Script for SelectTopNRows command from SSMS  ******/
SELECT  [electionDate],[jurisdiction],[description]
,[RijndaelKey],[RijndaelVector],[X509Data],[HMACKey]
  FROM [[redacted]].[dbo].[[redacted]Event]
```

	electionDate	jurisdiction	description	RijndaelKey	RijndaelVector	X509Data	HMACKey
1	2020-11-03	Maricopa County	General Election 2020	c$2[redacted]	7a$[redacted]	0x30[redacted]	0x455[redacted]

Source: Maricopa 2020 Database – Arizona Senate Audit

Second, it has been observed that the same password used since 2008 was publicly disclosed in a 2012 EAC report as a security issue. This concerns the accounts Techadvisor, MRO01, ROAdmin, and SAdmin. Furthermore, before the November 2020 election, the hash of this password was released online and subsequently decoded to "dvscorp08!". The discovery of the password hash

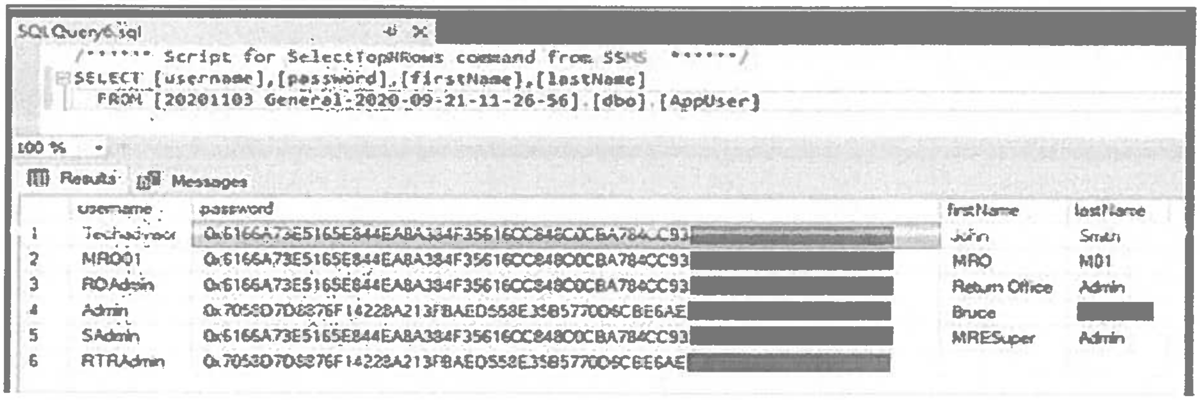
[1] Definition: RijndaelKey - Also known as Advanced Encryption Standard ("AES"), the key functions like a secret code used to lock and unlock data. AES uses these keys to scramble data so that only someone with the correct key can read it. Encrypting data means converting it into a secret code that can only be read with the correct key.

[2] Definition: RijndaelVector - an Initialization Vector ("IV") – An IV is a random number used along with the AES key. It ensures that if you encrypt the same data twice, it looks different each time. This randomness helps prevent certain types of attacks on the encrypted data. Unlike the encryption key, the IV does not need to be kept secret. However, it should be unique for each encryption operation with the same key. Reusing an IV with the same key can significantly weaken the security of the encryption.

[3] Definition: HMACKey - An HMAC key is used with a hashing algorithm to create a Hash-based Message Authentication Code. This code is used to verify both the data integrity and the authenticity of a message. HMAC involves a secret key shared between two parties.

online means that it is more than likely that a person has had access to the database or this password has been used on other sites that have been compromised by someone who reused the password.

Below is a screenshot of the password in un-decoded form for four different accounts:



```
/****** Script for SelectTopNRows command from SSMS  ******/
SELECT [username],[password],[firstName],[lastName]
  FROM [20201103 General-2020-09-21-11-26-56].[dbo].[AppUser]
```

	username	password	firstName	lastName
1	Techadmin	0x6166A73E5165E844EA8A384F35616CC848C0CBA784CC93[redacted]	John	Smith
2	MRO01	0x6166A73E5165E844EA8A384F35616CC848C0CBA784CC93[redacted]	MRO	M01
3	ROAdmin	0x6166A73E5165E844EA8A384F35616CC848C0CBA784CC93[redacted]	Return Office	Admin
4	Admin	0x7055D7D8876F14228A213FBAED558E35B57700SCBE6AE[redacted]	Bruce	[redacted]
5	SAdmin	0x6166A73E5165E844EA8A384F35616CC848C0CBA784CC93[redacted]	MRESuper	Admin
6	RTRAdmin	0x7053D7D8876F14228A213FBAED558E35B57700SCBE6AE[redacted]		

Source: Maricopa 2020 Database – Arizona Senate

VI. Potential Threats within the EMS

A. Advanced Encryption Standard (AES) "Rijndael"

Importantly, The Rijndael Key and Rinjdael Vector play a crucial role in the security of election systems. They are used to encrypt various critical files related to election processes, including:

- Election Files for ImageCast Precinct ("ICP") and election database ImageCast Evolution ("ICE"), These files likely contain configuration data and voter information relevant to the election.
- DCF ("ICP") and MBS ("ICE," "ICP2"): These could be specific files related to the election system's configuration and management.
- Result files ("ICE," "ICP2"): These files store the actual vote counts and other election results data.
- Reports and Logs: These documents likely contain audit trails, operational logs, and other records essential for verifying the integrity of the election.

Ultimately, if a malicious individual gains knowledge of the Rijndael Key and Vector specific to an election, the security implications would be catastrophic:

- Programming the Tabulators: A malicious actor accessing these keys could decrypt, alter, and re-encrypt the files used to program the tabulators. This could change how the tabulators record, count, or report votes, leading to fraudulent election results.
- Altering Election Results: Similarly, the individual could manipulate the results files. By decrypting these files, altering the vote counts or other data, and then re-encrypting imported by an unknowing actor and accepted by the EMS.

- The integrity of an election relies on the security of these cryptographic keys. It is imperative to ensure that these keys are protected against unauthorized access and that robust security practices are in place to prevent, detect, and respond to tampering or breaches.

B. Secure Connection to the NAS – Network Attached Storage

The same "ElectionEvent" table in the "20201103 General-2020-09-21-11-26-56" database from the Maricopa 2020 General election has a field called "x509Data." This data represents an X.509 Security Certificate.

X.509, certificated for encrypting traffic on a local network, particularly in the context of election systems, is an essential security measure. For example, the following scenarios are representative of a real-world application using the X.509 certificate:

- Ballot Image Transmission: When transferring ballot images from the ImageCast Central Tabulator for bulk scanning ballots or between the Election Management Server and Network Attached Storage, X.509 certificates provide a secure communication channel. This is crucial for maintaining the confidentiality and integrity of the ballot images.

- X.509 Certificates in Election Systems:

  a. Each X.509 certificate includes a public key and identity information (like a hostname or an organization name). This identity aspect is vital in an election context as it ensures the data is transmitted to and from trusted entities within the network.
  b. The certificates can be signed by a trusted Certificate Authority (CA) or self-signed. In a highly sensitive environment like an election system, certificates signed by a CA are preferable for added trust and security.
  c. TLS/SSL, which relies on X.509 certificates, encrypts the data in transit. This means that even if the network traffic is intercepted, the ballot images and results remain confidential and cannot be easily read or altered by unauthorized parties.

- Security Implications:

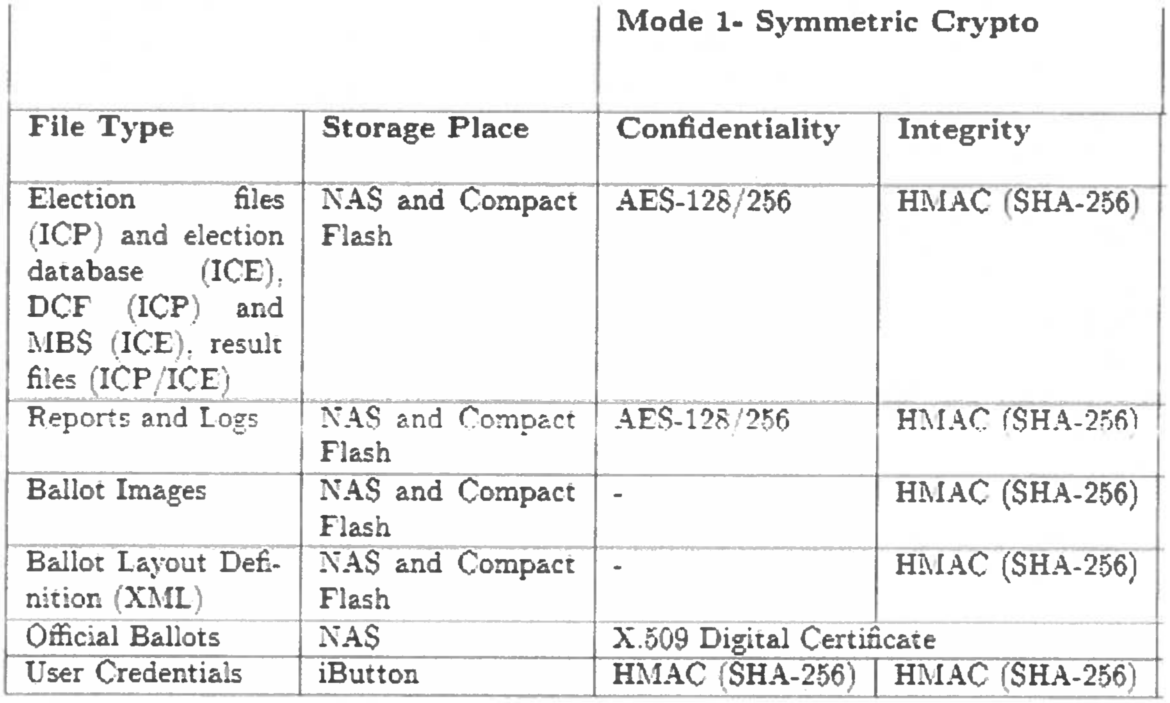
  a. Confidentiality: The encryption provided by X.509 certificates ensures that ballot images and results are kept confidential during transmission.
  b. Integrity: TLS/SSL protocols also provide integrity checks, ensuring that the data has not been tampered with during transit.
  c. Authentication: The identity verification aspect of X.509 helps authenticate the communicating parties and is a crucial method to prevent malicious actors from intercepting and altering data.

In summary, using X.509 data in election systems to encrypt network traffic is critical for ensuring the voting process remains secure and trustworthy. It safeguards against threats like eavesdropping, data tampering, and unauthorized access, which are paramount in preserving the integrity of elections.

C. Integrity and Security Risks in File Authentication and Access Control

The same "ElectionEvent" table in the "20201103 General-2020-09-21-11-26-56" database from the Maricopa 2020 General election has a field called "HMACkey." This is a Hash-based Message Authentication Code ("HMAC").

Dominion Graphic shows how these keys are used.



		Mode 1- Symmetric Crypto	
File Type	Storage Place	Confidentiality	Integrity
Election files (ICP) and election database (ICE), DCF (ICP) and MBS (ICE), result files (ICP/ICE)	NAS and Compact Flash	AES-128/256	HMAC (SHA-256)
Reports and Logs	NAS and Compact Flash	AES-128/256	HMAC (SHA-256)
Ballot Images	NAS and Compact Flash	-	HMAC (SHA-256)
Ballot Layout Definition (XML)	NAS and Compact Flash	-	HMAC (SHA-256)
Official Ballots	NAS	X.509 Digital Certificate	
User Credentials	iButton	HMAC (SHA-256)	HMAC (SHA-256)

File Type to Security Algorithmic Mappings

Source: MASTER SOLUTION PURCHASE AND SERVICES AGREEMENT BY AND BETWEEN DOMINION VOTING SYSTEMS, INC. as Contractor, and SECRETARY OF STATE OF THE STATE OF GEORGIA as State Dated as of July 29, 2019

- The HMAC key's role in election system integrity: The HMAC key is integral in verifying the integrity of various files within the election system. Dominion's documentation indicates its widespread use across files to ensure integrity. In this context, integrity assures that files have not been altered or tampered with. A compromised HMAC key means this layer of security is effectively nullified, allowing altered files to appear as though they are legitimate and unmodified.
- Programming User Credentials for iButtons: The HMAC key is used for file verification and is crucial in programming user credentials for iButtons. These iButtons are essentially electronic keys that allow authorized personnel to perform specific, often critical, operations on the tabulator systems. The security of the iButtons is paramount, as they hold the power to execute high-level commands within the election infrastructure. If the process of programming these iButtons is compromised, unauthorized individuals can alter an election result.

Ultimately, the security of the HMAC key is vital. Its compromise affects the integrity of documents and files within the election system. It allows a malicious actor to control the overall administration of the election process, including the programming of critical security tokens like iButtons. Ensuring the HMAC key is protected against unauthorized access is essential for maintaining the trustworthiness and security of the election process. Utilizing the HMAC key, a malicious individual or a program developed by such an individual could:

- Employ the HMAC key to sign altered files, fabricating fraudulent ballots, configuration files, and result files without likely detection.
- Replicate a security token, specifically an "iButton," used for administrative access and to implement modifications on a tabulator. Doing so allows a malicious actor to control and alter the tabulation of ballots without likely detection.

VII. Potential Threats from Malicious Actors in Election Systems

Considering the vulnerabilities identified within the EMS, understanding the threats posed by malicious actors, including insider threats, is crucial. These individuals can exploit the system's weaknesses to change an election outcome without being detected. The following scenarios depict various methods a malicious actor could use to rig an election. These scenarios range from tampering with the programming of voting equipment to manipulating final election results without likely detection.

- Tampering with Tabulator Programming: A malicious actor accessing the HMAC key can reprogram the tabulators. Modifying the tabulator's software or configuration files could alter how votes are counted or reported, leading to fraudulent election results. This could be done by creating fraudulent documents that appear legitimate due to the authentication of the HMAC key.
- Fabricating or Altering Ballot Images: By intercepting and decrypting the network traffic (using compromised X509 data), a bad actor can modify or replace the ballot images sent from scanning devices to the election management system. These altered images could falsely represent voter choices, impacting the election outcome.
- Creating Fake Security Tokens: If the HMAC keys for programming iButtons are compromised, a malicious individual could create unauthorized security tokens. These tokens can be used to gain administrative access to election systems, allowing the malicious actor to implement changes in the tabulation process or even access sensitive voter information.
- Manipulating Final Election Results: With knowledge of the Rijndael Key and Vector, a bad actor can decrypt, alter, and re-encrypt the result files before they are imported into the EMS. This manipulation would present falsified results as legitimate without likely detection.
- Unauthorized Access and Control Over Election Infrastructure: A malicious actor can gain extensive control over the election infrastructure by replicating or emulating security tokens and exploiting encryption keys. This includes changing the programming of tabulators, altering how votes are counted, or even turning off certain security features, making the system vulnerable to further attacks, again without likely detection.

VIII. Conclusion

The findings in the report of the team of cyber security experts reveal profound failures within Dominion's EMS. The ease with which passwords can be decrypted, the repeated use of outdated and compromised passwords, and the lack of stringent access controls and encryption key management reveal systemic weaknesses that can be exploited to produce fraudulent elections that would likely go undetected without a significant forensic examination of the voting system. Indeed, it is highly likely that many, if not most, election systems are currently compromised by either sleeper malware installed on the systems or are open to malicious actors who know where to look for the algorithmic decryption keys placed unprotected on every voting system we have inspected. A malicious actor's ability to compromise elections necessitates reactive measures in response to identified threats and a proactive and dynamic approach to election cybersecurity. With the advances of Artificial Intelligence ("LLMs"), knowledge to perform the tasks needed to manipulate election files is more accessible; skills that took years to learn can be asked as how-to questions, including writing code to perform the actions in the AI's answers.

IX. Request

Given the weaknesses within the EMS of the Dominion Democracy Suite 5.5-A, including those pertaining to cryptographic keys, the Rijndael Key and Vector, the X509 Certificate, and the HMAC, we respectfully request that the Secretary conduct a re-examination of the Dominion Democracy Suite 5.5-A and issue a report containing findings and conclusions with respect to that re-examination.

Affidavit of Clay U. Parikh

1. I am over twenty-one (21) years of age, under no legal disability, and am otherwise competent to give this affidavit.

2. The matters sworn to herein are based on my personal knowledge.

3. I have a Master of Science in Cyber Security, Computer Science from the University of Alabama in Huntsville. I have a Bachelor of Science in Computer Science, Systems Major from the University of North Carolina at Wilmington. In February 2007 I obtained the Certified Information Systems Security Professional (CISSP) certification and continually maintained good standing, until I released it on 28 February 2024. I also held the following certifications: Certified Ethical Hacker (CEH) and Certified Hacking Forensic Investigator (CHFI).

4. Since December of 2003, I have continually worked in the areas of Information Assurance (IA), Information Security and Cyber Security. I have performed and led teams in Vulnerability Management, Security Test and Evaluation (ST&E) and system accreditation. I have supported both civil and Department of Defense agencies within the U.S. government as well as international customers, such as NATO. I have served as the Information Security Manager for enterprise operations at Marshall Space Flight Center, where I ensured all NASA programs and projects aboard the center met NASA enterprise security standards. I was also responsible in part for ensuring the Marshall Space Flight Center maintained its Authority to Operate (ATO) within the NASA agency. I have also served as the Deputy Cyber Manager for the Army Corps of Engineers where I led and managed several teams directly in: Vulnerability Management, Assessment and Authorization (A&A), Vulnerability Scanning, Host Based Security System (HBSS), Ports Protocols and Service Management, and an Information System Security Manager (ISSM) team for cloud projects. I also have performed numerous internal digital forensic audits. During this time span, I also worked at the Army Threat Systems Management Office (TSMO) as a member of the Threat Computer Network Operations Team (TCNOT). I provided key Computer Network Operations (CNO) support by performing validated threat CNO penetration testing and systems security analysis. TCNOT is the highest

level of implementation of the CNO Team concept.

5. From 2008 to 2017, I also worked through a professional staffing company for several testing laboratories that tested electronic voting machines. These laboratories included Wyle Laboratories, which later turned into National Technical Systems (NTS) and Pro V&V. My duties were to perform security tests on vendor voting systems for the certification of those systems by either the Election Assistance Commission (EAC), or to a state's specific Secretary of State's requirements.

6. I have provided consultation and technical analysis on several Georgia election complaints and inquiries. In that effort I have reviewed voting system certification test reports, test plans, EAC relevant documents, and Georgia election laws and regulations.

7. While conducting analysis of several Dominion election databases, from various states, I obtained four Georgia county databases from the 2020 election. These databases had originally been obtained via Public Records Requests. The counties were Appling, Bibb, Jones, and Telfair.

8. The focus of that effort was to compare Arizona's election database to other Dominion databases in, Colorado, Georgia, Michigan, and Pennsylvania in preparation for my declaration to the U.S. Supreme Court. The scope of this effort was to further examine the Georgia databases.

EXECUTIVE SUMMARY

9. An ***egregious*** security violation has been discovered, relating to the cryptographic encryption keys utilized by the voting equipment provided and serviced by Dominion Voting Systems, Inc. ("Dominion"). Dominion placed these encryption keys on voting system election databases unprotected and in plain text in violation of EAC-certification requirements and its contract with the state of Georgia. Analysis of the four counties election databases (Appling, Bibb, Jones, and Telfair) confirmed this security violation.

10. The secret encryption key and x509 certificate used to encrypt, decrypt, the election data, and used for authentication when transferring files and communication are stored in plaintext, unprotected within the election database. Compounding this, the database is not

configured to standard security configurations used for a database dealing with sensitive information. These findings indicate that all cryptographic safeguards, designed to ensure the security and accuracy of election results and data, have been rendered meaningless.

11. Upon analysis and review of the four Georgia databases, each database contained simple and easy to guess passcodes, common or shared passwords were also discovered. One anomaly found was that the same exact security code was being utilized in other states during the same election period. The same password and/or security code for certain accounts are identical to the password or security code used in Maricopa County, AZ and Mesa County, CO.

12. Given my education, experience as a security professional and years of experience working with Voting System Testing Laboratories (VSTL), and the thorough analysis of the systems, processes, and the electronic records detailed above, the facts have led to the conclusion that the voters of Georgia should have no confidence that their votes have been accurately counted, if they were even counted at all.

DETAILED FINDINGS AND CONCLUSIONS

13. Dominion's Democracy Suite systems use a combination of a Rijndael Key, a Rijndael Vector, a Hash-based Message Authentication Code (HMAC) and a x509 security certificate to encrypt, decrypt and to authenticate data. The encryption key is considered a secret key and should be hidden and protected. All the components listed above (security processes) should be stored encrypted, especially if stored within a database. In the Democracy Suite systems, they are not. They are left unprotected and out in the open easy to find. See the figures for each county in **Exhibit A**.

14. The purpose of using encryption in election systems is to prevent unauthorized access to those systems and to prevent malicious alteration of election results. EAC-certification requirements mandate that these encryption keys must be kept secret from unauthorized access. With these items anyone could manipulate system configuration files causing the tabulators to not function properly. They could create or duplicate election data and make it look authentic. The possible attacks or manipulation of data are endless.

15. Furthermore, the plaintext storage of passwords and encryption keys on **any** information system, let alone a voting system, is an **egregious, inexcusable** violation of long-standing, **basic** cybersecurity best practices. It destroys any type of security the system wishes to implement. Windows log-in is the only authentication needed to access the unprotected database where the keys are stored. Windows log-in can easily be bypassed.[1]

16. Electronic voting systems overall are full of vulnerabilities with multiple exploits available. The vulnerabilities range from outdated Operating Systems (OS), third party applications, to protocols and services. Adding to these weaknesses is system configuration. Nearly all aspects of the voting systems do not use standard security, let alone industry best practices when configuring their systems. Voting system vendors, like Dominion, lack basic configuration management of their systems.

17. The election database is a prime example of misconfiguration. It is standard practice for a database to not use OS authentication to access or modify the database. Democracy Suite versions use OS authentication, which increases the number of attack vectors on the database. Additionally, if a database is to hold sensitive data it should be configured to encrypt the table, column, or row to which the sensitive data is to reside. This prevents anyone with read only or unauthorized access from seeing the data.

18. These keys being plaintext outside of the cryptographic module also **violates** FIPS 140-2. Section 4.7 of FIPS 140-2 "Cryptographic Key Management"[2] states "The security requirements for cryptographic key management encompass the entire lifecycle of cryptographic keys[.]" The section also states that "Secret keys, private keys, and CSPs shall be protected within the cryptographic module from unauthorized disclosure, modification, and substitution." Section 4.7.5 "Key Storage" states "Plaintext secret and private keys shall not be accessible from outside the cryptographic module to unauthorized operators." Additionally, the National Institute of Standards and Technology NIST SP 800-57[3] section 4.7 "Key Information Storage" states "The integrity of all key information **shall** be protected; the confidentiality of secret and

[1] https://www.youtube.com/watch?v=2v-mGf4_9-A
[2] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf pg.30
[3] https://doi.org/10.6028/NIST.SP.800-57pt2r1

private keys and secret metadata **shall** be protected. When stored outside a cryptographic module[.]"

19. Georgia law requires that the voting system be certified by the EAC. O.C.G.A. § 21-2-300 (2022). The EAC requires voting systems to be tested for compliance with the Voluntary Voting Systems Guidelines (VVSG). The VVSG specifically include requirements for storing cryptographic encryption keys, expressly adopting the Federal Information Processing Standards (FIPS) defining the mandatory practices and management of these keys to include storage of the keys in a cryptographic module or to be encrypted themselves.[4]

20. Of note regarding the technical and supervisor passcodes, the string of numbers repetitively used as a passcode in the Georgia voting systems was also the same **exact** passcode found and used in both Maricopa County, Arizona and Mesa County, Colorado. This commonly known, easy to guess passcode, which was used across multiple states, increases the risk of possible exploitation exponentially.

21. Another anomaly like the one mentioned above also exists with some of the administrative account passwords and security codes. The Georgia accounts either share the same password, security code or both with Maricopa and Mesa County. See figures B-1 and B-2 in **Exhibit B**. The blue arrows on these figures highlight the out of state counties that have the same credentials. This is highly suspicious but more importantly it is a security concern.

22. I reviewed Dominion's response to these revelations.[5] Dominion's statement that "*The claim that access to any single credential could affect the result of an election undetected is implausible and conspiratorial*" is misleading for three reasons:

- While access to a "single credential" as characterized by Dominion, would likely not be sufficient to manipulate an election, that is not the situation here. The Dominion voting systems are so ill configured and full of vulnerabilities that one single user credential could gain access to the database where the encryption keys are left

[4] VVSG 1.0 (2005) 7.4.5.1 https://www.eac.gov/sites/default/files/eac_assets/1/28/VVSG.1.0_Volume_1.PDF

[5] https://lawandcrime.com/supreme-court/kari-lake-to-scotus-hurry-up-the-2024-election-is-coming-and-dominion-voting-machines-need-to-be-banned/

unprotected and in plain text for the world to see.

- Access to these unprotected in plain text encryption keys provide the capability to unlock or manipulate other accounts.
- Lastly, the encryption keys provide the means with which to fabricate and/or manipulate election results, change the configuration of voting systems components such as the tabulator. Manipulation of election results could happen at any level; the tabulator, memory card, server, or database level, which would be accepted by the system as authenticated results.

23. Dominion's statement that "*Dominion's machines are fully certified by the U.S. Election Assistance Commission...*" is likewise misleading because EAC certification of a voting system is not strictly limited to its operation "as tested" and defined in the corresponding Scope of Conformance. EAC-certification is an operational standard which must be maintained within the specifications as defined in the VVSG throughout the use of the voting system. See, e.g., VVSG Sections 8.1 (discussing the conforming the system to meet VVSG and state and local requirements throughout the life of the system) and 9.5 (discussing establishment of procedures to resolve identified defects). Dominion's voting systems are not operating as tested and certified by the EAC.

24. Dominion is also not compliant with its contract with the state of Georgia for the reasons previously stated above concerning the encryption keys. Exhibit B to the Master Solution Purchase and Services Agreement Dominion states:

- Section 8. System Security Description "Dominion utilizes authentication and authorization protocols that meet EAC VVSG 2005 standards. In addition, Dominion's solution relies on industry-standard security features to ensure that the correct users based on a user role or group are granted the correct privileges."
- Section 8.3 Encryption configurations for both data at rest and data in motion "Data generated by the Democracy Suite platform is protected by the deployment of FIPS approved symmetric AES and asymmetric RSA encryption."
- Section 8.9 Secure Development Process "Data integrity and confidentiality is also

implemented according to NIST defined and FIPS validate procedures and algorithms."

None of these sections are being fulfilled with the voting system in its current state.

CONCLUSION

25. The analysis of the four Georgia county databases, the multitude of account and credential issues found, the numerous vulnerabilities associated with the voting system components leave the voting systems in Georgia lacking any system integrity. The encryption mechanisms and security certificates are left totally unprotected in a highly vulnerable system in violation of the VVSG and EAC certification requirements. The result of these critical faults, individually or collectively, means there is no way to know if votes cast in either 2020 or 2022 election were correctly recorded or tabulated. Also, as there is no evidence these issues and violations have been resolved, there is no way to know if the results for the 2024 election cycle will be correctly recorded or tabulated.

Sworn and subscribed to me
this 15 day of August 2024

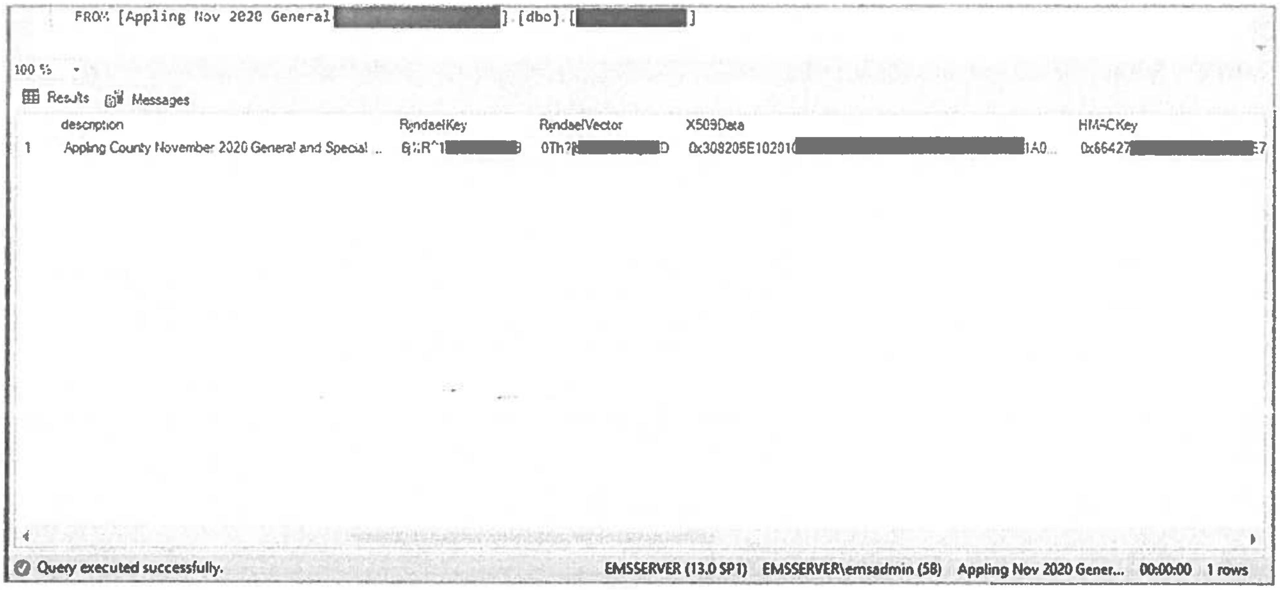
Clay U Parikh

Notary Public
My Commission Expires: My Commission Expires 05/21/2028

Clay U. Parikh

JACOB THORSON SMITH
NOTARY PUBLIC
ALABAMA STATE AT LARGE

Exhibit A

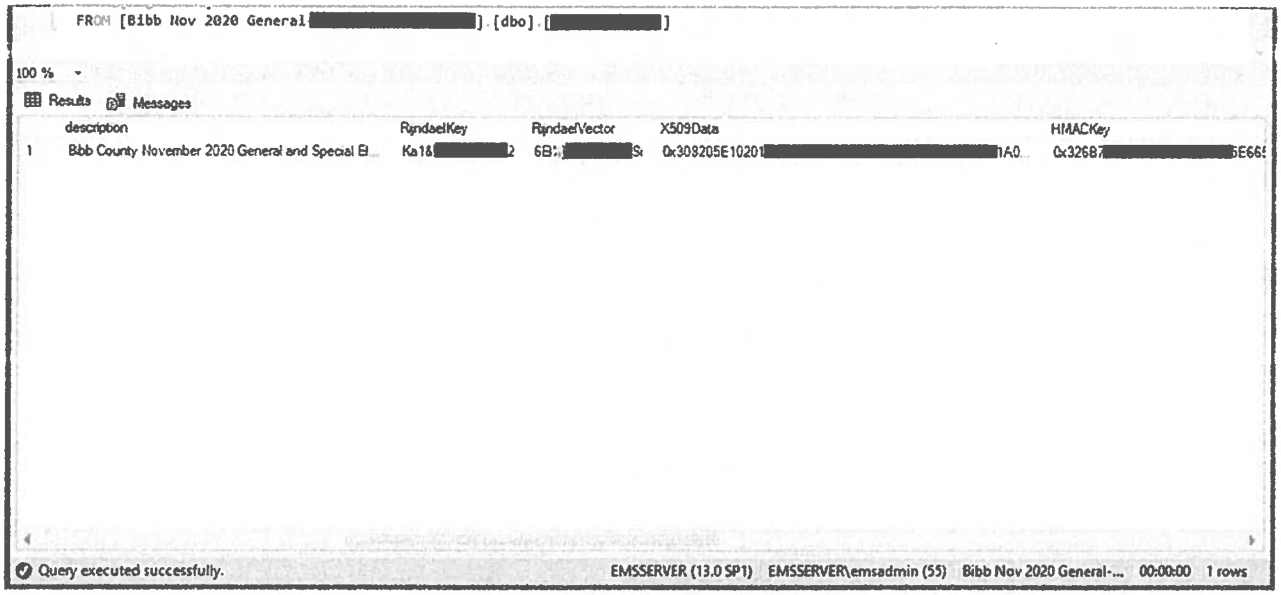


```
FROM [Appling Nov 2020 General[redacted]].[dbo].[[redacted]]
```

```
   description                                        RijndaelKey     RijndaelVector   X509Data                             HMACKey
1  Appling County November 2020 General and Special ...  6%R^1[redacted]9  0Th?[redacted]D  0x308205E10201[redacted]1A0...  0x66427[redacted]E7
```

```
Query executed successfully.   EMSSERVER (13.0 SP1)   EMSSERVER\emsadmin (58)   Appling Nov 2020 Gener...   00:00:00   1 rows
```

Figure A-1. Appling encryption keys

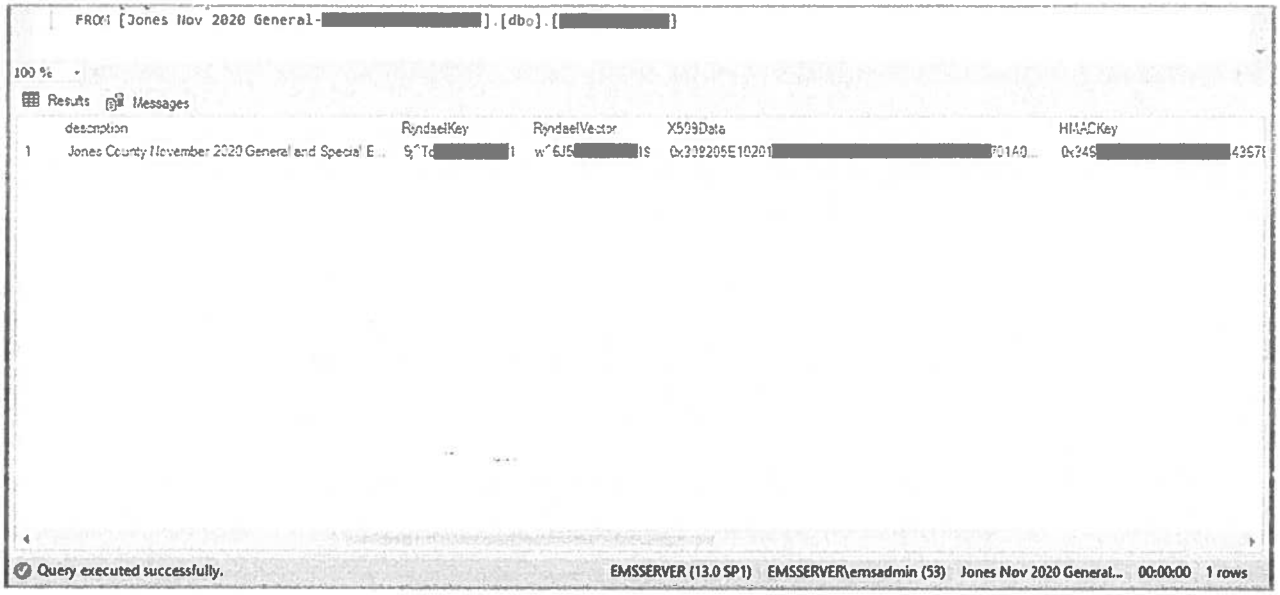


```
FROM [Bibb Nov 2020 General[redacted]].[dbo].[[redacted]]
```

```
   description                                        RijndaelKey     RijndaelVector   X509Data                             HMACKey
1  Bibb County November 2020 General and Special El...  Ka1&[redacted]2  6B:[redacted]S  0x308205E10201[redacted]1A0...  0x32687[redacted]5E665
```

```
Query executed successfully.   EMSSERVER (13.0 SP1)   EMSSERVER\emsadmin (55)   Bibb Nov 2020 General-...   00:00:00   1 rows
```

Figure A-2. Bibb encryption keys

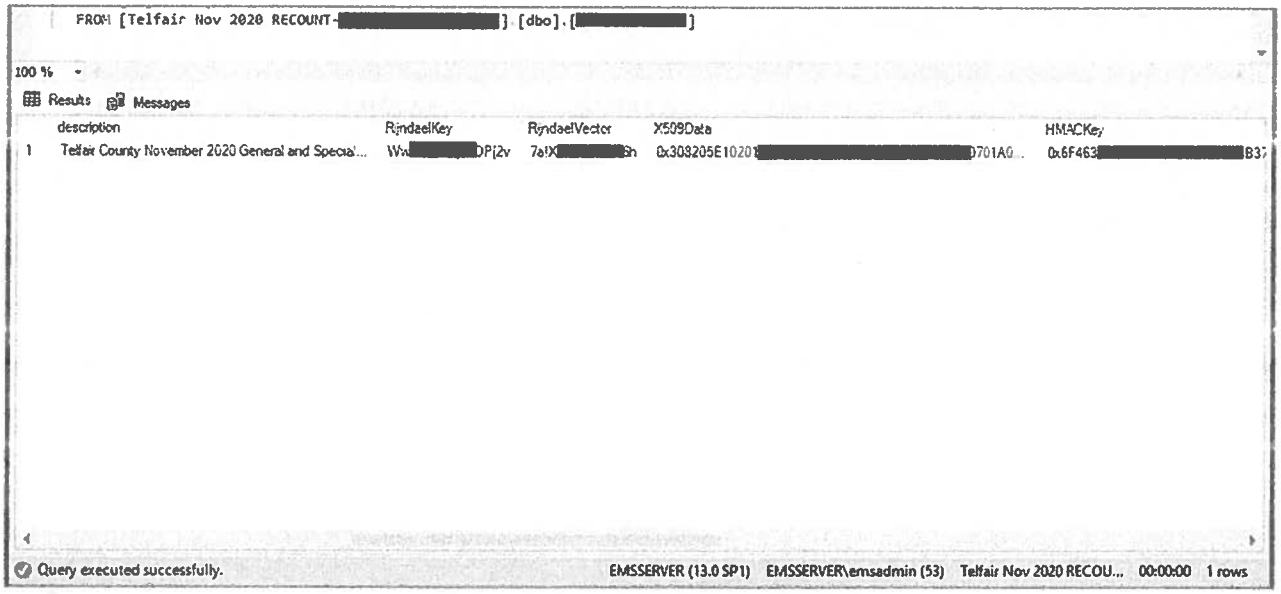


```
FROM [Jones Nov 2020 General-[redacted]].[dbo].[[redacted]]
```

```
   description                                       RijndaelKey    RijndaelVector   X509Data                                HMACKey
1  Jones County November 2020 General and Special E...  9^Td[redacted]1   w^6J5[redacted]1S    0x308205E10201[redacted]F01A0...    0x345[redacted]4357E
```

```
Query executed successfully.        EMSSERVER (13.0 SP1)   EMSSERVER\emsadmin (53)   Jones Nov 2020 General...   00:00:00   1 rows
```

Figure A-3. Jones encryption keys



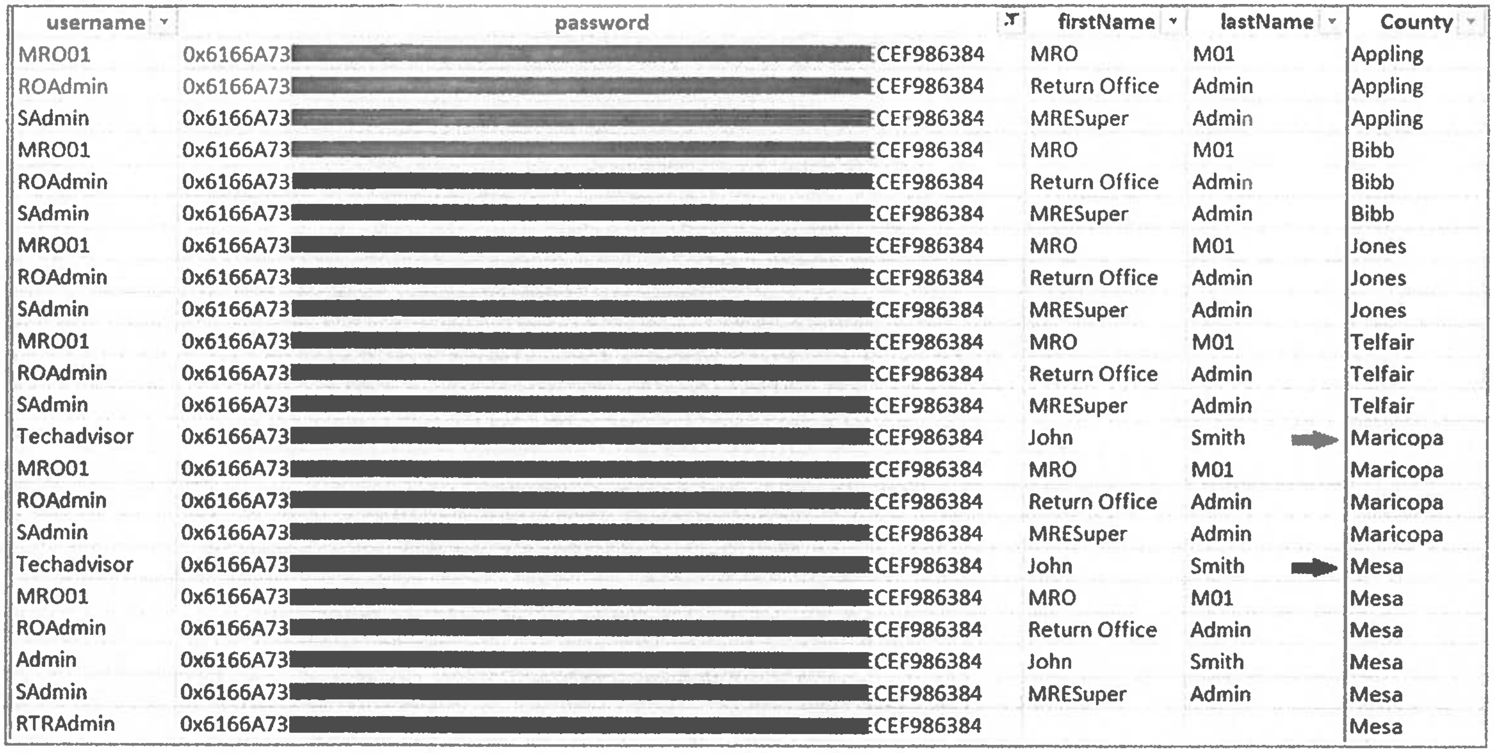
```
FROM [Telfair Nov 2020 RECOUNT-[redacted]].[dbo].[[redacted]]
```

```
   description                                     RijndaelKey      RijndaelVector   X509Data                                HMACKey
1  Telfair County November 2020 General and Specia'...  Ww[redacted]DP{2v   7a!X[redacted]6h     0x308205E10201[redacted]0701A0...   0x6F463[redacted]B37
```

```
Query executed successfully.        EMSSERVER (13.0 SP1)   EMSSERVER\emsadmin (53)   Telfair Nov 2020 RECOU...   00:00:00   1 rows
```

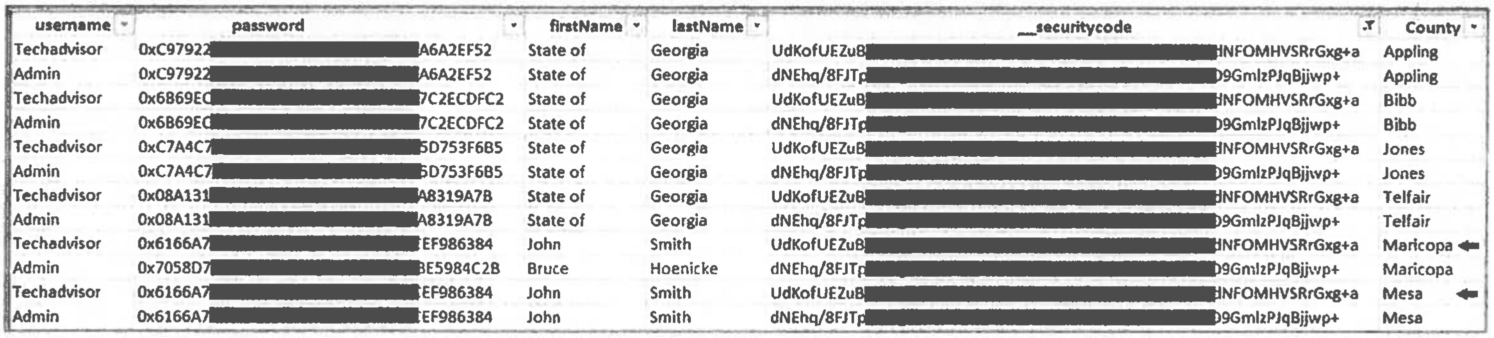
Figure A-4. Telfair encryption keys

Exhibit B



username	password	firstName	lastName	County
MRO01	0x6166A73[redacted]CEF986384	MRO	M01	Appling
ROAdmin	0x6166A73[redacted]CEF986384	Return Office	Admin	Appling
SAdmin	0x6166A73[redacted]CEF986384	MRESuper	Admin	Appling
MRO01	0x6166A73[redacted]CEF986384	MRO	M01	Bibb
ROAdmin	0x6166A73[redacted]CEF986384	Return Office	Admin	Bibb
SAdmin	0x6166A73[redacted]CEF986384	MRESuper	Admin	Bibb
MRO01	0x6166A73[redacted]CEF986384	MRO	M01	Jones
ROAdmin	0x6166A73[redacted]CEF986384	Return Office	Admin	Jones
SAdmin	0x6166A73[redacted]CEF986384	MRESuper	Admin	Jones
MRO01	0x6166A73[redacted]CEF986384	MRO	M01	Telfair
ROAdmin	0x6166A73[redacted]CEF986384	Return Office	Admin	Telfair
SAdmin	0x6166A73[redacted]CEF986384	MRESuper	Admin	Telfair
Techadvisor	0x6166A73[redacted]CEF986384	John	Smith ➡	Maricopa
MRO01	0x6166A73[redacted]CEF986384	MRO	M01	Maricopa
ROAdmin	0x6166A73[redacted]CEF986384	Return Office	Admin	Maricopa
SAdmin	0x6166A73[redacted]CEF986384	MRESuper	Admin	Maricopa
Techadvisor	0x6166A73[redacted]CEF986384	John	Smith ➡	Mesa
MRO01	0x6166A73[redacted]CEF986384	MRO	M01	Mesa
ROAdmin	0x6166A73[redacted]CEF986384	Return Office	Admin	Mesa
Admin	0x6166A73[redacted]CEF986384	John	Smith	Mesa
SAdmin	0x6166A73[redacted]CEF986384	MRESuper	Admin	Mesa
RTRAdmin	0x6166A73[redacted]CEF986384			Mesa

Figure B-1. Common Passwords



username	password	firstName	lastName	__securitycode	County
Techadvisor	0xC97922[redacted]A6A2EF52	State of	Georgia	UdKofUEZuB[redacted]dNFOMHVSRrGxg+a	Appling
Admin	0xC97922[redacted]A6A2EF52	State of	Georgia	dNEhq/8FJTp[redacted]D9GmlzPJqBjjwp+	Appling
Techadvisor	0x6B69EC[redacted]7C2ECDFC2	State of	Georgia	UdKofUEZuB[redacted]dNFOMHVSRrGxg+a	Bibb
Admin	0x6B69EC[redacted]7C2ECDFC2	State of	Georgia	dNEhq/8FJTp[redacted]D9GmlzPJqBjjwp+	Bibb
Techadvisor	0xC7A4C7[redacted]5D753F6B5	State of	Georgia	UdKofUEZuB[redacted]dNFOMHVSRrGxg+a	Jones
Admin	0xC7A4C7[redacted]5D753F6B5	State of	Georgia	dNEhq/8FJTp[redacted]D9GmlzPJqBjjwp+	Jones
Techadvisor	0x08A131[redacted]A8319A7B	State of	Georgia	UdKofUEZuB[redacted]dNFOMHVSRrGxg+a	Telfair
Admin	0x08A131[redacted]A8319A7B	State of	Georgia	dNEhq/8FJTp[redacted]D9GmlzPJqBjjwp+	Telfair
Techadvisor	0x6166A7[redacted]EF986384	John	Smith	UdKofUEZuB[redacted]dNFOMHVSRrGxg+a	Maricopa ⬅
Admin	0x7058D7[redacted]BE5984C2B	Bruce	Hoenicke	dNEhq/8FJTp[redacted]D9GmlzPJqBjjwp+	Maricopa
Techadvisor	0x6166A7[redacted]EF986384	John	Smith	UdKofUEZuB[redacted]dNFOMHVSRrGxg+a	Mesa ⬅
Admin	0x6166A7[redacted]EF986384	John	Smith	dNEhq/8FJTp[redacted]D9GmlzPJqBjjwp+	Mesa

Figure B-2. Common Security Codes

Affidavit of Benjamin Cotton

1) I am over twenty-one (21) years of age, under no legal disability, and am otherwise competent to give this affidavit.

2) The matters sworn to herein are based on my personal knowledge.

3) I am the founder of CyFIR, LLC (CyFIR) and Cyber Technology Services, INC.

4) I have a Master's Degree in Information Technology Management from the University of Maryland University College. I have numerous technical certifications, including the Certified Information Systems Security Professional (CISSP), Microsoft Certified Professional (MCP), Network+, and Certified CyFIR Forensics and Incident Response Examiner.

5) I have over twenty-seven (27) years of experience performing computer forensics and other digital systems analysis.

6) I have over twenty (20) years of experience as an instructor of computer forensics and incident response. This experience includes thirteen (13) years of experience teaching students on the Guidance Software (now OpenText) EnCase Investigator and EnCase Enterprise software.

7) I have testified as an expert witness in state courts, federal courts and before the United States Congress.

8) I regularly lead engagements involving digital forensics, cyber security, and incident response for law firms, corporations, and government agencies and am experienced with the digital acquisition of evidence under the Federal Rules of Evidence.

9) In the course of my duties, I have forensically examined Dominion Voting Systems (DVS) components in Maricopa County Arizona, Antrim County Michigan, Fulton County Pennsylvania,

Coffee County Georgia, Mesa County Colorado. These system components are hereinafter referred to as the "Analyzed Election County Components".

10) In the course of my duties I have examined Dominion voting databases from the 2020 elections produced pursuant to public records requests from Appling County, Bibb County, Jones County, and Telfair County. These counties are located in the State of Georgia, hereinafter referred to as the "Analyzed Election Databases".

11) In the course of my duties, I have reviewed the administrative manuals and documentation for the DVS Democracy Suite software and hardware components.

12) In the course of my duties, I have reviewed the public information from the Election Assistance Commission ("EAC") and its certification process for election software.

13) In the course of my duties I have reviewed the report dated 1 July 2021 by Alex J. Halderman titled "Security Analysis of Georgia's ImageCast X Ballot Marking Devices".

EXECUTIVE SUMMARY

14) I performed a thorough analysis of the Analyzed Election County Components and Analyzed Election Databases and have determined that the encryption keys used to secure the results, encrypt and decrypt the tabulator results and protect the integrity of the EMS operations are stored in plain text in an unencrypted SQL database that is accessible with a simple SQL query. This egregious security lapse provides anyone with access to the voting system with the tools to alter election results without likely detection.

15) The State of Georgia knew about critical vulnerabilities in the ability of the Dominion Voting Systems to secure the encryption keys vital to ensuring the integrity of Georgia's elections in July of 2021 and have failed to address any of the vulnerabilities.

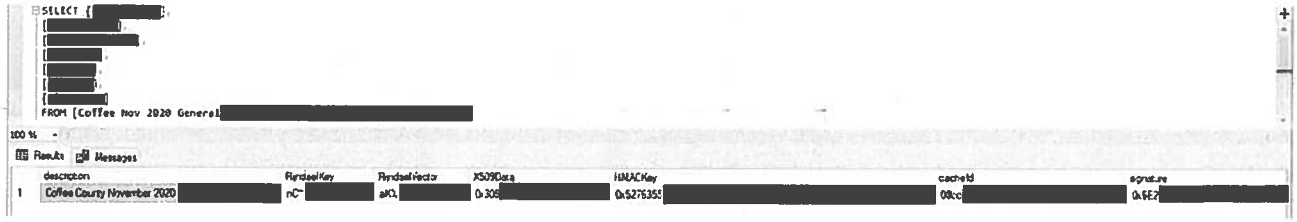
16) The Coffee County EMS has a compiler installed that provides the ability to modify and create executable files and drivers on the fly that could be used to alter election results without

detection. There is evidence that executable files were created and modified after the Dominion Voting Software (DVS) was installed and certified.

DETAILED FINDINGS

Unprotected Encryption Keys

17) In the course of my analysis, I determined that there was a flagrant failure to protect the election encryption and decryption keys within the election databases in the Analyzed County Election Components. The DVS Democracy Suite utilizes a combination of a Rijndael Key, a Rijndael Vector, a Hash-based Message Authentication Code (HMAC) and a x509 security certificate to encrypt, decrypt and authenticate data. This data includes code signing, data signing, communications, and tabulator results from ICC or ICP2 components. The protection of election encryption and decryption keys is prominently described by DVS within Democracy Suite Technical Data Package documents as the mitigation for the risk of a malicious actor tampering with the election database, election result files, scanned ballot images, device audit logs, device log reports, ballot definitions and other critical elements that could allow authorized or unauthorized parties, to alter the outcome of an election without detection. These keys have been left unprotected on the election database and are in plain text as shown below:



```
SELECT [redacted]
FROM [Coffee Nov 2020 General[redacted]
```

	description	RijndaelKey	RijndaelVector	X509Data	HMACKey	cacheId	signature
1	Coffee County November 2020 [redacted]	nC~[redacted]	aK\[redacted]	0x30[redacted]	0x5276355[redacted]	08cc[redacted]	0x6E2[redacted]

Figure 1 - Rijndael Key for Coffee County GA 2020 Election

18) The only barrier to access these keys is the Windows-log-in. Given the egregious lack of current cyber security precautions on the Analyzed Election Components, this log in obviously would not prevent a malicious actor from changing results. An actor could easily bypass the

Windows log-in feature in about 5 minutes with well-known hacking techniques available on the internet. Given the cyber security vulnerabilities, including the sharing of passwords between user accounts, access to all of these encryption elements is easily obtained. The encryption elements are stored in the MS SQL election database and are easily retrieved with a simple SQL query.

19) Simply put, this is like a bank having the most secure vault in the world, touting how secure it is to the public and then taping the combination in large font type on the wall next to the vault door. Anyone with local or remote access to the system, including authorized or unauthorized users, can obtain the certificates and keys and once obtained the entire election can be compromised. A simple example of the exploitation of these keys would be the modification of the results and .dvd files that are transmitted or copied from the ICC scanners, HiPro scanners and the ICP2 tabulators prior to the ingestion of these files into the EMS for counting. By leveraging the decryption/encryption keys it is possible to script a program that would automatically change the contents of the ICP2 tabulator .dvd files, results.txt and cast vote records files prior to ingestion into the EMS. This altered vote count would not be logged as an intrusion or an error. Simply put, it would not be detected on the EMS. As long as these keys are exposed and unprotected, the results of any election conducted on these systems can not be guaranteed.

20) It is clear from my review of the Alex J. Halderman report dated 1 July 2021 and titled ""Security Analysis of Georgia's ImageCast X Ballot Marking Devices" that the state of Georgia knew about the lack of protections of the encryption keys in the DVS ImageCast. Sections 6.1 and 6.2 detail in depth how to extract the keys from the cards used to authenticate to the ImageCast X (ICX) and acknowledges that access to these keys allows the changing of critical voting files including election results. There is no indication that these critical weaknesses in voting system security have been addressed.

The Georgia Voting Systems Contain the Ability to Modify and Create Executable Files and Drivers on the Fly

21) In computing, a compiler is a computer program that translates computer code, such as source code, to create an executable program that a computer can 'run'. These executable programs can be the common filename.exe format, but also include device drivers with the .dll extension as well as other forms of lower level executable code. In order to ensure that no erroneous code is present on voting systems, the Election Assistance Commission (EAC) establishes a 'scope of conformance' that contains a list of the hashes for the Dominion Voting System software that undergoes the certification process. This is to ensure that no executable program or device driver is later created or modified. Changing or modifying the executable programs and device drivers should invalidate the EAC certification and decertify the system, but more importantly could change the expected behaviors of the system, be used to create malicious programs on the system, create or open external communications, or modify election results. In order to create or modify an executable file or driver the programmer must use a compiler. Analysis of the Coffee County Election Management System (EMS) determined that it contained eight (8) different versions of the Microsoft compiler named MSbuild.exe. These compilers were present on the system at the time of the 2020 election and are present now[1]. The MD5 hash values for these eight different compilers are 3b2790718535d05f209a542d05575dda, 3c03b4467059c385b175aeaacc228391, 88144380e37cea1e1fd2aee3568bb27e, 88de8fbbd91803eef67064b39d702650, 8dbf81c4ad4a899790bd325bed966aff, 913f5dbfb11f4d590670821e4da28c2b, 9e40eeeb04222dfa5f2f43f39b171ba3, and fc6370d7bd71895b795da0fb75c26985. None of these compilers are contained in the EAC Scope of Conformance.

[1] There is no public acknowledgement or announcement that any modifications or updates have been made to the Dominion Democracy Suite 5.5A acquired by Georgia and used in the 2020 elections.

22) Analysis of the Coffee County EMS further determined that one thousand nine hundred ninety one (1,991) executable files were created after the installation of the Dominion Voting System on 9/12/2019. One thousand one hundred seven (1,107) executable files were modified after the installation of the Dominion Voting System on 9/12/2019. None of these hash values for the executable files created or modified after 9/12/2019 are contained in the EAC Scope of Conformance for the certification of the Dominion 5.5A voting system. Had there been any effective monitoring of the files on the accredited system, this system should have been decertified for use in elections.

23) I have had the opportunity to examine Dominion Voting Systems in Arizona, Georgia, Michigan and Pennsylvania. The MSBuild.exe compiler has been present in all the examined systems. It is reasonable to believe that the MSBuild.exe compiler exists on all Georgia voting systems.

24) The current methodology of the EAC approved auditors is flawed in that it only checks for changes to a specific filename that is located in a specific file path. Based on my analysis the methodology does not check for new or modified executable files or drivers.

CONCLUSION

25) The presence of compilers on the system and placing the master cryptographic keys on the election database in plain text and unprotected allows any actor with access to the voting system complete control over the election results. Any changes to the voting results leveraging these keys would likely not be detected. This is an egregious breach of basic security practices that must be remedied immediately. No election results provided by these voting machines can be trusted given the subjects identified and described in this report. The fact that these vulnerabilities have not been addressed places the integrity and outcome of any election at risk.

SIGNED UNDER THE PAINS AND PENALTIES OF PERJURY THIS 18th DAY OF AUGUST, 2024.

Benjamin R. Cotton

Sworn to and subscribed before me, this 18th day of August, 2024.

Notary Public
My commission expires: 9/29/27

KEANNA KRUEGER
COMMISSION EXPIRES
NOTARY
23037336
PUBLIC
9-29-27
STATE OF WASHINGTON

State of Washington
County of Kittitas
Signed and sworn to (or affirmed) before me on
8/18/24 by Keanna Krueger

Notary Public

Appendix B – EAC Certification Scope

CertConf_Scope_DSuite5.5-A.pdf

United States Election Assistance Commission

VVSG 2005 VER. I

EAC

CERTIFIED

Certificate of Conformance

Dominion Voting Systems
Democracy Suite 5.5-A

The voting system identified on this certificate has been evaluated at an accredited voting system testing laboratory for conformance to the *Voluntary Voting System Guidelines Version 1.0 (VVSG 1.0)* . Components evaluated for this certification are detailed in the attached Scope of Certification document. This certificate applies only to the specific version and release of the product in its evaluated configuration. The evaluation has been verified by the EAC in accordance with the provisions of the EAC *Voting System Testing and Certification Program Manual* and the conclusions of the testing laboratory in the test report are consistent with the evidence adduced. This certificate is not an endorsement of the product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.

Product Name: Democracy Suite

Model or Version: 5.5-A

Name of VSTL: SLI Compliance

EAC Certification Number: DVS-DemSuite5.5-A

Date Issued: January 30, 2019

Executive Director

Scope of Certification Attached

Manufacturer: *Dominion Voting Systems (DVS)*
System Name: *Democracy Suite 5.5-A*
Certificate: *DVS-DemSuite5.5-A*

Laboratory: *SLI Compliance*
Standard: *VVSG 1.0 (2005)*
Date: *January 30, 2019*

Scope of Certification

This document describes the scope of the validation and certification of the system defined above. Any use, configuration changes, revision changes, additions or subtractions from the described system are not included in this evaluation.

Significance of EAC Certification

An EAC certification is an official recognition that a voting system (in a specific configuration or configurations) has been tested to and has met an identified set of Federal voting system standards. An EAC certification is **not**:

- An endorsement of a Manufacturer, voting system, or any of the system's components.
- A Federal warranty of the voting system or any of its components.
- A determination that a voting system, when fielded, will be operated in a manner that meets all HAVA requirements.
- A substitute for State or local certification and testing.
- A determination that the system is ready for use in an election.
- A determination that any particular component of a certified system is itself certified for use outside the certified configuration.

Representation of EAC Certification

Manufacturers may not represent or imply that a voting system is certified unless it has received a Certificate of Conformance for that system. Statements regarding EAC certification in brochures, on Web sites, on displays, and in advertising/sales literature must be made solely in reference to specific systems. Any action by a Manufacturer to suggest EAC endorsement of its product or organization is strictly prohibited and may result in a Manufacturer's suspension or other action pursuant to Federal civil and criminal law.

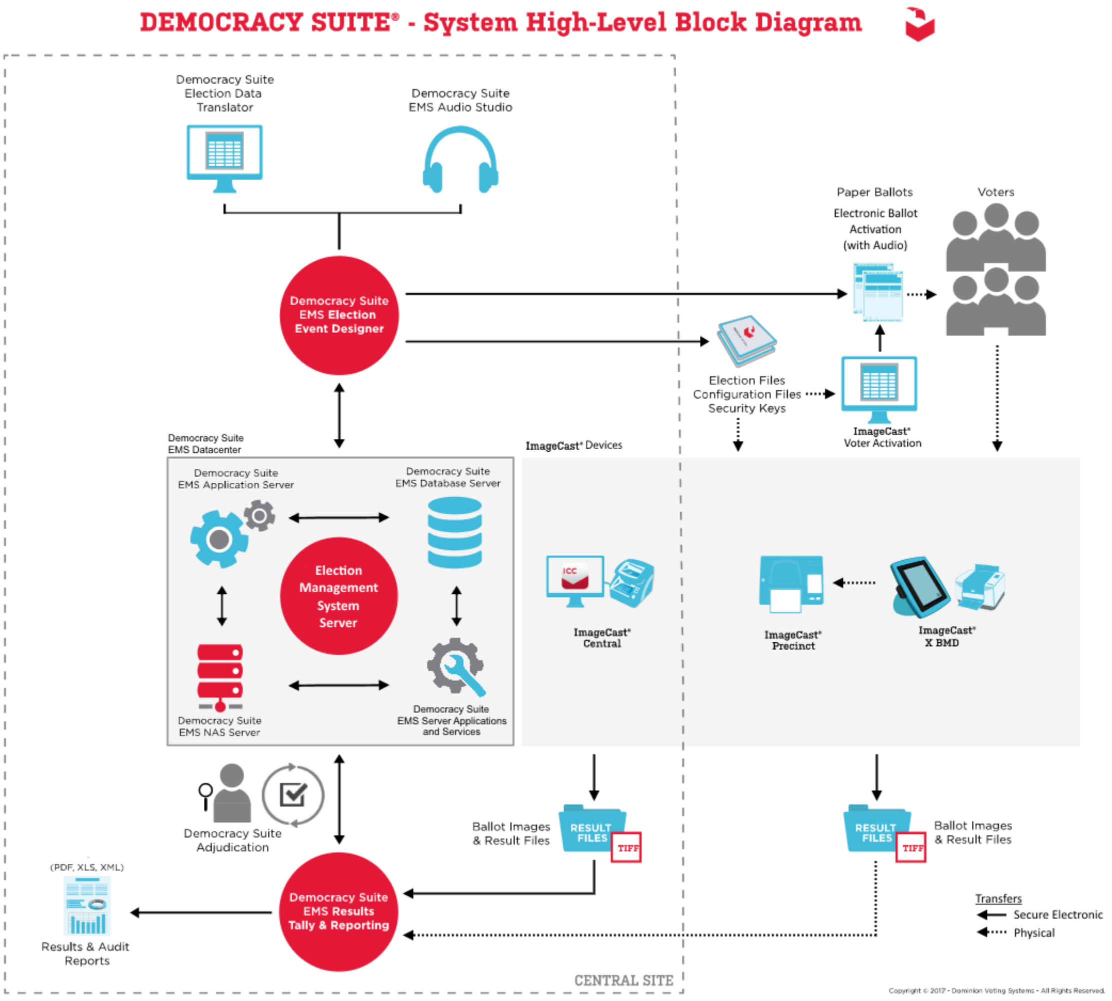
System Overview:

The D-Suite 5.5-A Voting System is a paper-based optical scan voting system with a hybrid paper/DRE option consisting of the following major components: The Election Management System (EMS), the ImageCast Central (ICC), the ImageCast Precinct (ICP), and the ImageCast X ballot marking device (BMD). The D-Suite 5.5-A Voting System configuration is a modification from the EAC approved D-Suite 5.5 system configuration.

Language capability:

System supports Alaska Native, Apache, Bengali, Chinese, English, Eskimo, Filipino, French, Hindi, Japanese, Jicarilla, Keres, Khmer, Korean, Navajo, Seminole, Spanish, Thai, Towa, Ute, Vietnamese, and Yuman.

Democracy Suite 5.5-A System Diagram


DEMOCRACY SUITE® - System High-Level Block Diagram
Democracy Suite Election Data Translator
Democracy Suite EMS Audio Studio
Democracy Suite EMS Election Event Designer
Paper Ballots
Electronic Ballot Activation (with Audio)
Voters
Election Files Configuration Files Security Keys
ImageCast® Voter Activation
Democracy Suite EMS Datacenter
ImageCast® Devices
Democracy Suite EMS Application Server
Democracy Suite EMS Database Server
Election Management System Server
Democracy Suite EMS NAS Server
Democracy Suite EMS Server Applications and Services
ICC
ImageCast® Central
ImageCast® Precinct
ImageCast® X BMD
Democracy Suite Adjudication
Ballot Images & Result Files
RESULT FILES
TIFF
RESULT FILES
TIFF
Ballot Images & Result Files
(PDF, XLS, XML)
Results & Audit Reports
Democracy Suite EMS Results Tally & Reporting
CENTRAL SITE
Transfers
Secure Electronic
Physical
Copyright © 2017 - Dominion Voting Systems - All Rights Reserved.

Components Included:

This section provides information describing the components and revision level of the primary components included in this Certification.

Voting System Software Components:

System Component	Software or Firmware Version	Operating System or COTS	Comments
EMS Election Event Designer (EED)	5.5.12.1	Windows 10 Pro	EMS
EMS Results Tally and Reporting (RTR)	5.5.12.1	Windows 10 Pro	EMS
EMS Application Server	5.5.12.1	Windows Server 2012 R2 Windows 10 Pro	EMS
EMS File System Service (FSS)	5.5.12.1	Window 10 Pro	EMS
EMS Audio Studio (AS)	5.5.12.1	Windows 10 Pro	EMS
EMS Data Center Manager (DCM)	5.5.12.1	Windows Server 2012 R2 Windows 10 Pro	EMS
EMS Election Data Translator (EDT)	5.5.12.1	Windows 10 Pro	EMS
ImageCast Voter Activation (ICVA)	5.5.12.1	Windows 10 Pro	EMS
EMS Adjudication (ADJ)	5.5.8.1	Windows 10 Pro	EMS
EMS Adjudication Services	5.5.8.1	Windows 10 Pro	EMS
Smart Card Helper Service (SCHS)	5.5.12.1	Windows 10 Pro	EMS
Election Firmware	5.5.3-0002	uClinux	ICP
Firmware Updater	5.5.3-0002	uClinux	ICP
Firmware Extractor	5.5.3-0002	uClinux	ICP
Kernel (uClinux)	5.5.3-0002	Modified COTS	ICP
Boot Loader (COLILO)	20040221	Modified COTS	ICP
Asymmetric Key Generator	5.5.3-0002	uClinux	ICP
Asymmetric Key Exchange Utility	5.5.3-0002	uClinux	ICP
Firmware Extractor (Technician Key)	5.5.3-0002	uClinux	ICP
ImageCast Central Application	5.5.3.0002	Windows 10 Pro	ICC
ICX Application	5.5.10.30	Android 5.1 (ICX Prime)	ICX

Voting System Platform:

System Component	Version	Operating System or COTS	Comments
Microsoft Windows Server	2012 R2 Standard	Unmodified COTS	EMS Server SW Component
Microsoft Windows	10 Professional	Unmodified COTS	EMS Client/Server SW Component
.NET Framework	3.5	Unmodified COTS	EMS Client/Server SW Component
Microsoft Visual J#	2.0	Unmodified COTS	EMS Client/Server SW Component
Microsoft Visual C++ 2013 Redistributable	2013	Unmodified COTS	EMS Client/Server SW Component
Microsoft Visual C++ 2015 Redistributable	2015	Unmodified COTS	EMS Client/Server SW Component
Java Runtime Environment	7u80	Unmodified COTS	EMS Client/Server SW Component
Java Runtime Environment	8u144	Unmodified COTS	EMS Client/Server SW Component

System Component	Version	Operating System or COTS	Comments
Microsoft SQL Server 2016Standard	2016 Standard	Unmodified COTS	EMS Client/Server SW Component
Microsoft SQL Server 201 Service Pack 2	2016 SP1	Unmodified COTS	EMS Client/Server SW Component
Microsoft SQL Server 2016 SP1 Express	2016 SP1	Unmodified COTS	EMS Client/Server SW Component
Cepstral Voices	6.2.3.801	Unmodified COTS	EMS Client/Server SW Component
Arial Narrow Fonts	2.37a	Unmodified COTS	EMS Client/Server SW Component
Maxim iButton Driver	4.05	Unmodified COTS	EMS Client/Server SW Component
Adobe Reader DC	AcrobatDC	Unmodified COTS	EMS Client/Server SW Component
Microsoft Access Database Engine	2010	Unmodified COTS	EMS Client/Server SW Component
Open XML SDK 2.0 for Microsoft Office	2.0	Unmodified COTS	EMS Client/Server SW Component
Infragistics NetAdvantage Win Forms 2011.1	2011 Vol. 1	Unmodified COTS	EMS SW Platform
Infragistics NetAdvantage WPF 2012.1	2012 Vol. 1	Unmodified COTS	EMS SW Platform
TX Text Control Library for .NET	16.0	Unmodified COTS	EMS SW Platform
SOX	14.3.1	Unmodified COTS	EMS SW Platform
NLog	1.0.0.505	Unmodified COTS	EMS SW Platform
iTextSharp	5.0.5	Unmodified COTS	EMS SW Platform
OpenSSL	1.0.2K	Unmodified COTS	EMS SW Platform
OpenSSL FIPS Object Module	2.0.14 (Cert 1747)	Unmodified COTS	EMS SW Platform
SQLite	1.0.103.0	Unmodified COTS	EMS SW Platform
Lame	3.99.4	Unmodified COTS	EMS SW Platform
Speex	1.0.4	Unmodified COTS	EMS SW Platform
Ghostscript	9.04	Unmodified COTS	EMS SW Platform
One Wire API for .NET	4.0.2.0	Unmodified COTS	EMS SW Platform
Avalon-framework-cvs-20020806	20020806	Unmodified COTS	EMS SW Platform
Batik	0.20-5	Unmodified COTS	EMS SW Platform
Fop	0.20-5	Unmodified COTS	EMS SW Platform
Microsoft Visual J# 2.0 Redistributable Package – Second Edition (x64)	2.0	Unmodified COTS	EMS SW Platform
Entity framework	6.1.3	Unmodified COTS	EMS SW Platform
Spreadsheetlight	3.4.3	Unmodified COTS	EMS SW Platform
Open XML SDK 2.0 for Microsoft Office	2.0.5022.0	Unmodified COTS	EMS SW Platform
Open SSL	1.0.2K	Unmodified COTS	ICP
OpenSSL FIPS Object Module	2.0.10 (Cert 1747)	Unmodified COTS	ICP
Zlib	1.2.3	Unmodified COTS	ICP
uClinux	20070130	Modified COTS	ICP
Google Text-to-Speech Engine	3.11.12	Unmodified COTS	ICX SW
Zxing Barcode Scanner	4.7.5	Modified COTS	ICX SW
SoundTouch	1.9.2	Modified COTS	ICX SW
ICX Prime Android 5.1.1 Image	0405	Modified COTS	ICX SW
ICX Classic Android 4.4.4 Image	0.0.98	Modified COTS	ICX SW
OpenSSL FIPS Object Module	2.0.10 (Cert 2473)	Unmodified COTS	ICX SW Build Library

System Component	Version	Operating System or COTS	Comments
OpenSSL	1.0.2K	Unmodified COTS	ICC SW Build Library
OpenSSL FIPS Object Module	2.0.10 (Cert 1747)	Unmodified COTS	ICC SW Build Library
1-Wire Driver (x86)	4.05	Unmodified COTS	ICC Runtime SW
1-Wire Driver (x64)	4.05	Unmodified COTS	ICC Runtime SW
Canon DR-G1130 Driver	1.2 SP6	Unmodified COTS	ICC Runtime SW
Canon DR-G1130 TWAIN Driver	1.2 SP6	Unmodified COTS	ICC Runtime SW
Visual C++ 2013 Redistributable (x86)	12.0.30501	Unmodified COTS	ICC Runtime SW
Machine Configuration File (MCF)	5.5.10.19_20180706	Proprietary	ICX Configuration File
Device Configuration File (DCF)	5.4.01_20170521	Proprietary	ICP and ICC Configuration File

Hardware Components:

System Component	Hardware Version	Proprietary or COTS	Comments
ImageCast Precinct (ICP)	PCOS-320C	Proprietary	Hybrid Precinct Scanner/DRE
ImageCast Precinct (ICP)	PCOS-320A	Proprietary	Hybrid Precinct Scanner/DRE
ICP Ballot Box	BOX-330A	Proprietary	Ballot Box
ICP Ballot Box	BOX-340C	Proprietary	Ballot Box
ICP Ballot Box	BOX-341C	Proprietary	Ballot Box
ICX UPS Inline EMI Filter	1.0	Proprietary	EMI Filter
ICX Tablet (Classic)	aValue 21” Tablet (SID-21V)	COTS	Ballot Marking Device
ICX Tablet (Prime)	aValue 21” Tablet (HID-21V)	COTS	Ballot Marking Device
Server	Dell PowerEdge R630	COTS	Standard Server
Server	Dell PowerEdge R640	COTS	Standard Server
Server	Dell Precision T3420	COTS	Express Server
ICC Workstation HW	Dell OptiPlex 7440 All in One	COTS	
ICC Workstation HW	Dell OptiPlex 9030 All In One	COTS	
ICC Workstation HW	Dell OptiPlex 3050 All In One	COTS	
ICC Scanner	Canon imageFormula DR-G1130	COTS	Central Count Scanner
ICC Scanner	Canon imageFormula DR-M160II	COTS	Central Count Scanner
Client Workstation HW	Dell Precision T3420	COTS	
Client Workstation HW	Dell Latitude E7450	COTS	
Client Workstation HW	Dell Latitude e3480	COTS	
ICX Printer	HP LaserJet Pro Printer M402dn	COTS	
ICX Printer	HP LaserJet Pro Printer M402dne	COTS	
Monitor	Dell Monitor KM632	COTS	
Monitor	Dell Monitor P2414Hb	COTS	
Monitor	Dell Ultrasharp 24” Monitor U2414H	COTS	
CD/DVD Reader	Dell DVD Multi Recorder GP60NB60	COTS	
iButton Programmer	Maxim iButton Programmer DS9490R# with DS1402	COTS	
UPS	APC Smart-UPS SMT1500	COTS	
Network Switch	Dell X1008	COTS	
Network Switch	Dell X1018	COTS	

System Component	Hardware Version	Proprietary or COTS	Comments
Network Switch	Dell X1026	COTS	
Network Switch	Dell PowerConnect 2808	COTS	
Sip and Puff	Enabling Devices Sip and Puff	COTS	
Headphones	Cyber Acoustics ACM-70	COTS	
4-way Joystick Controller	S26	Modified COTS	
Rocker (Paddle) Switch	Enablemart #88906	COTS	
Footswitches	ABLENET Jelly Bean Twist 10033400	COTS	
CF Card Reader	IOGEAR SDHC/microSDHC 0U51USC410	COTS	
CF Card Dual-Slot Reader	Lexar USB 3.0	COTS	
CF Card Reader	Hoodman Steel USB 3.0 102015	COTS	
CF Card Reader	Lexar Professional CFR1	COTS	
CF Card Reader	Kingston FCR-HS4	COTS	
ATI	ATI handset	Proprietary	
ATI	ATI-USB handset	Proprietary	
ACS PC-Linked Smart Card Reader	ACR39U	COTS	

System Limitations

This table depicts the limits the system has been tested and certified to meet.

Characteristic	Limiting Component	Limit	Comment
Ballot positions	Ballot	292*/462**	Both
Precincts in an election	EMS	1000; 250	Standard; Express
Contests in an election	EMS	1000; 250	Standard; Express
Candidates/Counters in an election	EMS	10000; 2500	Standard; Express
Candidates/Counters in a precinct	Ballot	240*/462**	Both
Candidates/Counters in a tabulator	Tabulator	10000; 2500	Standard; Express
Ballot Styles in an election	Tabulator	3000; 750	Standard; Express
Ballot IDs in a tabulator	Tabulator	200	Both
Contests in a ballot style	Ballot	38*/156**	Both
Candidates in a contest	Ballot	240*/231**	Both
Ballot styles in a precinct	Tabulator	5	Both
Number of political parties	Tabulator	30	Both
“vote for” in a contest	Ballot	24*/30**	Both
Supported languages in an election	Tabulator	5	Both
Number of write-ins	Ballot	24*/462**	Both

* Reflects the system limit for a ballot printed in landscape.

** Reflects the system limit for a ballot printed in portrait.

Functionality

2005 VVSG Supported Functionality Declaration

Feature/Characteristic	Yes/No	Comment
Voter Verified Paper Audit Trails		
VVPAT	NO	
Accessibility		
Forward Approach	YES	
Parallel (Side) Approach	YES	
Closed Primary		
Primary: Closed	YES	
Open Primary		
Primary: Open Standard (provide definition of how supported)	YES	
Primary: Open Blanket (provide definition of how supported)	YES	
Partisan & Non-Partisan:		
Partisan & Non-Partisan: Vote for 1 of N race	YES	
Partisan & Non-Partisan: Multi-member ("vote for N of M") board races	YES	
Partisan & Non-Partisan: "vote for 1" race with a single candidate and write-in voting	YES	
Partisan & Non-Partisan "vote for 1" race with no declared candidates and write-in voting	YES	
Write-In Voting:		
Write-in Voting: System default is a voting position identified for write-ins.	YES	
Write-in Voting: Without selecting a write in position.	NO	
Write-in: With No Declared Candidates	YES	
Write-in: Identification of write-ins for resolution at central count	YES	
Primary Presidential Delegation Nominations & Slates:		
Primary Presidential Delegation Nominations: Displayed delegate slates for each presidential party	YES	
Slate & Group Voting: one selection votes the slate.	YES	
Ballot Rotation:		
Rotation of Names within an Office; define all supported rotation methods for location on the ballot and vote tabulation/reporting	YES	Equal time rotation
Straight Party Voting:		
Straight Party: A single selection for partisan races in a general election	YES	
Straight Party: Vote for each candidate individually	YES	
Straight Party: Modify straight party selections with crossover votes	YES	
Straight Party: A race without a candidate for one party	YES	
Straight Party: "N of M race (where "N">1)	YES	
Straight Party: Excludes a partisan contest from the straight party selection	YES	
Cross-Party Endorsement:		
Cross party endorsements, multiple parties endorse one candidate.	YES	
Split Precincts:		
Split Precincts: Multiple ballot styles	YES	

Feature/Characteristic	Yes/No	Comment
Split Precincts: P & M system support splits with correct contests and ballot identification of each split	YES	
Split Precincts: DRE matches voter to all applicable races.	YES	
Split Precincts: Reporting of voter counts (# of voters) to the precinct split level; Reporting of vote totals is to the precinct level	YES	
Vote N of M:		
Vote for N of M: Counts each selected candidate, if the maximum is not exceeded.	YES	
Vote for N of M: Invalidates all candidates in an overvote (paper)	YES	
Recall Issues, with options:		
Recall Issues with Options: Simple Yes/No with separate race/election. (Vote Yes or No Question)	YES	
Recall Issues with Options: Retain is the first option, Replacement candidate for the second or more options (Vote 1 of M)	NO	
Recall Issues with Options: Two contests with access to a second contest conditional upon a specific vote in contest one. (Must vote Yes to vote in 2nd contest.)	NO	
Recall Issues with Options: Two contests with access to a second contest conditional upon any vote in contest one. (Must vote Yes to vote in 2nd contest.)	NO	
Cumulative Voting		
Cumulative Voting: Voters are permitted to cast, as many votes as there are seats to be filled for one or more candidates. Voters are not limited to giving only one vote to a candidate. Instead, they can put multiple votes on one or more candidate.	NO	
Ranked Order Voting		
Ranked Order Voting: Voters can write in a ranked vote.	NO	
Ranked Order Voting: A ballot stops being counting when all ranked choices have been eliminated	NO	
Ranked Order Voting: A ballot with a skipped rank counts the vote for the next rank.	NO	
Ranked Order Voting: Voters rank candidates in a contest in order of choice. A candidate receiving a majority of the first choice votes wins. If no candidate receives a majority of first choice votes, the last place candidate is deleted, each ballot cast for the deleted candidate counts for the second choice candidate listed on the ballot. The process of eliminating the last place candidate and recounting the ballots continues until one candidate receives a majority of the vote	NO	
Ranked Order Voting: A ballot with two choices ranked the same, stops being counted at the point of two similarly ranked choices.	NO	
Ranked Order Voting: The total number of votes for two or more candidates with the least votes is less than the votes of the candidate with the next highest number of votes, the candidates with the least votes are eliminated simultaneously and their votes transferred to the next-ranked continuing candidate.	NO	

Feature/Characteristic	Yes/No	Comment
Provisional or Challenged Ballots		
Provisional/Challenged Ballots: A voted provisional ballots is identified but not included in the tabulation, but can be added in the central count.	YES	
Provisional/Challenged Ballots: A voted provisional ballots is included in the tabulation, but is identified and can be subtracted in the central count	NO	
Provisional/Challenged Ballots: Provisional ballots maintain the secrecy of the ballot.	YES	
Overvotes (must support for specific type of voting system)		
Overvotes: P & M: Overvote invalidates the vote. Define how overvotes are counted.	YES	Overvotes cause a warning to the voter and can be configured to allow voter to override.
Overvotes: DRE: Prevented from or requires correction of overvoting.	YES	
Overvotes: If a system does not prevent overvotes, it must count them. Define how overvotes are counted.	YES	If allowed via voter override, overvotes are tallied separately.
Overvotes: DRE systems that provide a method to data enter absentee votes must account for overvotes.	N/A	
Undervotes		
Undervotes: System counts undervotes cast for accounting purposes	YES	
Blank Ballots		
Totally Blank Ballots: Any blank ballot alert is tested.	YES	Precinct voters receive a warning; both precinct and central scanners will warn on blank ballots.
Totally Blank Ballots: If blank ballots are not immediately processed, there must be a provision to recognize and accept them	YES	Blank ballots are flagged. These ballots can be manually examined and then be scanned and accepted as blank; or precinct voter can override and accept.
Totally Blank Ballots: If operators can access a blank ballot, there must be a provision for resolution.	YES	Operators can examine a blank ballot, re-mark if needed and allowed, and then re-scan it.
Networking		
Wide Area Network – Use of Modems	NO	
Wide Area Network – Use of Wireless	NO	
Local Area Network – Use of TCP/IP	YES	Client/server only
Local Area Network – Use of Infrared	NO	

Feature/Characteristic	Yes/No	Comment
Local Area Network – Use of Wireless	NO	
FIPS 140-2 validated cryptographic module	YES	
Used as (if applicable):		
Precinct counting device	YES	ImageCast Precinct
Central counting device	YES	ImageCast Central

Baseline Certification Engineering Change Orders (ECO)

There are no ECOs applied to this modification that are not certified as part of the baseline Democracy Suite 5.5 voting system.