

IN THE SUPERIOR COURT OF FULTON COUNTY

STATE OF GEORGIA

DEKALB COUNTY REPUBLICAN PARTY, INC.

APPLICANT,

v.

BRAD RAFFENSPERGER, IN HIS OFFICIAL
CAPACITY AS THE SECRETARY OF STATE OF
THE STATE OF GEORGIA,

RESPONDENT

Civil Action File No.

24CV011028

APPLICATION FOR WRIT OF MANDAMUS

COME NOW, the DeKalb County Republican Party, Inc., and, pursuant to O.C.G.A. § 9-3-20 et seq., brings this Application for writ of mandamus for relief against Brad Raffensperger in his Official Capacity as the Secretary of State of the State of Georgia as follows:

INTRODUCTION

1.

As detailed below, Georgia uses election computer systems manufactured by Dominion Voting Systems ("Dominion.") The Dominion system used in Georgia and elsewhere uses cryptographic encryption keys to secure election systems to prevent unauthorized access to those systems and the malicious alteration of code, data and election results. Georgia law requires that these systems be certified by the Election

election results. Georgia law requires that these systems be certified by the Election Assistance Commission (“EAC”). EAC certification requirements mandate that the cryptographic encryption keys be protected from unauthorized access by placing them in a cryptographic module in accordance with Federal Information Processing Standards (“FIPS”). Georgia’s Dominion’s systems violate that certification requirement by placing the encryption keys on its election systems in an unprotected state and in plain text within county election systems readable to anyone with licit or illicit access to the system.

The Secretary of State has been on notice of this violation of EAC certification requirements since at least March 28, 2024 when one of the undersigned counsel informed the Secretary of State’s General Counsel, Charlene McGowan, on March 28, 2024 via email. McGowan acknowledge receipt of that email by in a responsive email dated April 11, 2024. Among other things, the Secretary of State’s failure to enforce the mandatory requirement that Georgia’s election systems be EAC certification-compliant has compromised all passwords and administrative level controls on Georgia’s election systems. Particularly concerning is that four Georgia counties produced election data for the 2020 election pursuant to open records requests issued more than two years ago, which data has been lawfully published online. The encryption keys for these counties’ systems are included in these public records disclosures, and the administrator and technician passwords are also accessible to the public. In short, the Secretary of State’s

failure to enforce mandatory security requirements for encryption keys has compromised Georgia's election systems and left them vulnerable to any malicious actor – foreign or domestic – to manipulate election results without likely detection.

PARTIES, JURISDICTION AND VENUE

2.

The DeKalb County Republican Party, Inc. ("DeKalb GOP") is a Georgia non-profit corporation with its principal office in DeKalb County, Georgia. DeKalb GOP is a political organization—duly registered with the Secretary of State pursuant to O.C.G.A. § 21-2-111. As set forth in its bylaws, it exists "to promote the Republican principles and policies adopted by the Georgia Republican Party in convention and further the aims of the National Republican Party platform." The DeKalb GOP aims to support and ensure the election of Republican candidates in free and fair elections conducted according to law. As a membership organization whose members are candidates and voters in elections in Georgia, the DeKalb GOP is entitled to the due and proper enforcement and application of Georgia's Election Code, and to the conduct of elections on voting systems that comply with the requirements of Georgia law.

3.

Marci McCarthy is a citizen of DeKalb County, Georgia. She is also a member and the Chair of the DeKalb GOP. She has a professional background in cyber security.

4.

Under Georgia's Election Code, the Secretary of State is the Chief Elections Official of the State of Georgia. O.C.G.A. § 21-2-50(b).

5.

Sovereign immunity does not apply to mandamus relief.

6.

The Secretary of State may be served by service of process upon the Secretary of State, Attention: General Counsel, 214 State Capitol, Atlanta, Georgia 30334.

7.

Venue and jurisdiction over this case lie in Fulton Superior Court because the Executive Office of the Secretary of State is located in Fulton County.

STANDING

8.

The DeKalb GOP has a legally cognizable injury sufficient to support a claim for mandamus relief arising from the State's mandating the use of election systems that do not meet the cyber security requirements of Georgia law as described below. The DeKalb GOP therefore has organizational standing to bring this action as the complained of conduct by the Secretary of directly affects its organizational interests and purposes and as a community stakeholder as contemplated by O.C.G.A. § 9-6-24. *See also Sons of Confederate Veterans v. Henry County Board of Commissioners*, 315 Ga. 39,

57-60 (2022). Alternatively, the DeKalb GOP has associational standing to bring this case on behalf of its 123 voting members who are registered voters, residents and citizens of DeKalb County. Some of its members have been, presently are, or in the future will be candidates for office, whose interests are cognizably injured by the State's mandating the use of election systems that do not meet the cyber security requirements of Georgia law as community stakeholders as contemplated by O.C.G.A. § 9-6-24 as described below in that:

(a) Its individual members would otherwise have standing to bring this action in their own right;

(b) The interests that DeKalb GOP seeks to protect in this action are germane to its purposes of preserving liberty under law, including through the election to office of Republican candidates in free and fair elections conducted according to law. The DeKalb GOP, as a member of the Georgia Republican Party, supports the interests identified by the Georgia Republican Party's Election Confidence Task Force, see <https://gagop.org/election-confidence-task-force/> (last visited Aug. 26, 2024); and

(c) Neither the claim asserted nor the relief requested requires the participation of individual members in this action.

FACTS

9.

The State of Georgia, by statute and through the Secretary of State, mandates that Georgia counties use Dominion's "Democracy Suite" platform to conduct elections.

10.

As detailed below, the Dominion system mandated by the State uses master (private) cryptographic encryption keys to secure Georgia's election systems. The purpose of using encryption in election systems is to prevent unauthorized access to those systems and to prevent malicious alteration of election results. These encryption keys must be kept secret from unauthorized access to comply with express requirements mandated by Georgia law, the EAC and the terms of the Master Solution Purchase and Services Agreement with Dominion for the purchase of their system of election machines and services (the "Contract") ("Exh. 1"). In violation of Georgia law and the Contract, the Dominion system mandated by the State not only stores the encryption keys on its election systems in a non-compliant unprotected state, it leaves them in plain text within the election databases on county systems. In this condition, anyone with access to the voting system or the transmission of election results can alter election results without likely detection.

11.

The encryption keys provide access to the various encrypted files, passwords, and election records and data used by the Dominion voting system vital to counting and reporting votes in an accurate, secure and reliable manner, including .dvd files, .sha files, results files, etc. With the encryption keys, these encrypted files can be decrypted and then edited, modified and re-encrypted without corresponding entries in the system log files, making the alterations substantially undetectable.

12.

On or about July 29, 2019, the Secretary of State, on behalf of the State, entered into the Contract with Dominion for the purchase of electronic voting equipment and the terms of the Contract remain in force today. The Secretary of State's representatives have admitted under oath that his office outsourced security for its election systems to Dominion, meaning that Dominion, a third party non-governmental entity, has *total control over Georgia's elections* by, among other things, its unfettered access to these encryption keys. See *Curling v. Raffensperger*, Trial Transcript Vol. 5A, p. 109.

13.

Georgia law, O.C.G.A. § 21-2-300(a)(3), requires that the voting system used be certified by the EAC:

The state shall furnish a uniform system of electronic ballot markers and ballot scanners for use in each county as soon as possible. Such equipment shall be certified by the United States Election Assistance Commission prior to purchase, lease, or acquisition.

14.

For federal certification, the EAC requires voting systems to be tested for compliance with the Voluntary Voting Systems Guidelines (“VVSG”). In other words, to achieve certification, compliance with these guidelines becomes mandatory, not voluntary or discretionary. The VVSG specifically include the requirements for data encryption, and also adopt the Federal Information Processing Standards (“FIPS”) defining the mandatory practices for management of cryptographic keys. In particular, VVSG 1.0 (2005) requires “cryptographic keys ... use a FIPS 140-2 level 1 or higher validated cryptographic module.” VVSG § 7.4.5.1(a)(i), p. 122, Hashes and Digital Signatures. *See also id.*, § 7.5.1(b)(i), p. 125, Maintaining Data Integrity; § 7.7.3(a)(ii), p. 132, Protecting Transmitted Data; and § 7.9.3, p. 138, Electronic and Paper Record Structure subsection a. VVSG 1.0 (2005) is available here:

https://www.eac.gov/sites/default/files/eac_assets/1/28/VVSG.1.0_Volume_1.PDF (last visited Aug. 29, 2024).

15.

EAC certification is not a static event or merely a matter of form. The VVSG requires ongoing compliance with its requirements including correction of any deficiencies that become known. *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).

16.

In its Contract with the State, Dominion represents that “Dominion implements security protocols that meet or exceed EAC VVSG 2005 requirements. All of Dominion’s security protocols are designed and implemented to stay current with the rapidly evolving EAC security requirements set forth by various iterations of the VVSG.” Exh. B to Contract, section 8. Further, the Contract requires that “[d]ata generated by the Democracy Suite platform is protected by the deployment of FIPS-approved symmetric AES and asymmetric RSA encryption.” (*Id.*, section 8.3). The Contract also requires the Dominion system to “*meet all Mandatory Requirements*” and “*accurately function in accordance with those requirements... enabling State and all other State Entities to accurately and securely administer elections throughout the State of Georgia in accordance with Applicable Laws of the State of Georgia.*” Contract at § 1.2 (emphasis added). The Dominion Contract also represents that “In addition, proper system and software hardening procedures are clearly defined and regularly tested. Data integrity and confidentiality is also implemented according to NIST defined and FIPS validate procedures and algorithms” *Id.*, Exh. B to Contract, § 8.9.

17.

Dominion itself admitted in an internal email that “From an engineering perspective, the main reason why we don’t want unencrypted databases is that then the

integrity of the election data and results cannot be guaranteed.” Exh. 2. About that, Dominion is exactly right.

18.

In plain violation of the mandatory requirements of State law, EAC certification and the incorporated requirements of the VVSG and FIPS 140-2, in the Dominion systems in use in Georgia the master (private) cryptographic encryption keys are placed in the election database unprotected (other than the Windows log-in which is easily bypassed by tools available on e.g., YouTube) and in plain text within the election database. Storing the master cryptographic keys in this insecure and unencrypted fashion makes them available to anyone who has remote or onsite access to log on to the system (e.g., Dominion employees, hackers, anyone onsite from authorized staff). This insecure storage of the encryption keys is a dangerous and plain violation of the above-referenced requirements of Georgia law and of EAC certification and of the contract between the State and Dominion. Indeed, as stated above, FIPS 140-2 expressly requires that cryptographic encryption keys be stored within a cryptographic module to protect them from unauthorized access.

19.

This insecure and improper plain text storage of the encryption keys has been confirmed in every 2020 election database that Applicant and its consultants have examined, and includes those from the following Georgia jurisdictions:

- a. Appling County, Georgia,
- b. Bibb County, Georgia,
- c. Coffee County, Georgia,
- d. Jones County, Georgia, and
- e. Telfair County, Georgia.

20.

Copies of the Appling, Bibb, Jones, and Telfair County election databases were lawfully obtained via an Open Records Act request and are available on the internet as of October 2021. The election databases contain the master encryption keys described herein stored in an insecure manner as described above. Any member of the public can now decrypt the administrative and technician passwords for these counties' election systems using these unprotected cryptographic encryption keys, and with access to these counties' systems (either on-site or remote) can now take total control of these voting machines and the election results.

21.

A nefarious actor may also have already exploited these vulnerabilities in multiple ways. For example, malicious code may have been placed on Georgia's election systems that could modify the electronic tallies at will, change the running code on these systems, and compromise the integrity and outcome of an election without detection. Even if not previously exploited, a malicious actor could take the same actions with respect to the upcoming 2024 election and alter the election results. The

encryption keys provide access to the system tools necessary to escape detection, especially by a sophisticated attacker such as a hostile nation state with a powerful interest in the outcome of the election.

22.

White hat researchers have successfully and lawfully performed these manipulations in a lab setting forensically identical to those in use by Georgia county election offices, with frightening ease. Georgia's election system by design "trusts" the encrypted files stored on the memory card or from a directory on the EMS server, and implicitly accepts the results from such files without any other restrictive qualification. Thus, for example, the Results Tally and Reporting ("RTR") application on the Dominion system requires a separate Secure Hash Algorithm ("SHA") hash value equal to the SHA hash value of the results being submitted, without regard to the actual provenance or authenticity of those results. In other words, it is only the encryption of the results that in normal operation protects against falsely validated and fabricated results. The keys provide the capability to defeat this protection by encrypting bogus files which the application by design accepts as authorized and authentic. With these encryption keys a malicious actor can alter the results of an election merely by dragging and dropping manipulated results and replacing the actual recorded results of an election.

23.

As a result of the foregoing, the Dominion systems used in Georgia do not comply with O.C.G.A. § 21-21-300(a)(3), which, as noted above, requires certification by the EAC, which certification requirements also require ongoing compliance with the VVSG requirements for data encryption discussed above. Nor are these voting systems “safe and practicable for use” as required by O.C.G.A. § 23-2-300(a)(2) and Ga. Comp. R. & Regs. 590-8-1-.01 (“3. The intent of these Rules is to assure that hardware, firmware, and software have been shown to be reliable, accurate, and capable of secure operation before they are used in elections in the State.”).

24.

Competent and qualified expert testimony regarding the nature and gravity of the cyber security failures described herein is as follows:

(a) Clay Parikh performed EAC-certification testing for the Voting System Testing Laboratories accredited by the EAC for a period of nine (9) years, including Pro V&V, the very laboratory which tested Georgia’s voting system for certification. Parikh Dec. ¶ 5.¹ Parikh testified as follows:

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

¹ Affidavit of Clay Parikh attached as Exh. 3.

(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.

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 longstanding, **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.

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" 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 "Plain text 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 800-573 section 4.7 "Key Information Storage" states "The integrity of all key information **shall** be protected; the confidentiality of secret and private keys and secret metadata **shall** be protected. When stored outside a cryptographic module[.]"

(Emphasis in original, footnotes omitted).

(b) Cyber-security and forensics expert Benjamin Cotton testified as follows:

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:

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.*²

(Emphasis added).

(c) In *Curling v. Raffensperger*, U.S.D.C. N.D. Ga., Case No. 1:17-CV-2989-AT (Curling), Professor J. Alex Halderman of the University of Michigan prepared a lengthy expert report dated July 1, 2021 entitled "Security Analysis of Georgia's ImageCast X Ballot Marking Devices" ("Halderman Report") analyzing the cyber security vulnerabilities of one component of the Dominion elections system. This report revealed such alarming security failures in the voting system that Judge Totenberg, presiding in *Curling*, placed the report under seal while it was under review by the

² Affidavit of Ben Cotton attached as Exh. 4.

Cybersecurity Infrastructure Security Agency (“CISA”). The Halderman Report was later unsealed in redacted form.³ Professor Halderman identified the insecure storage of encryption keys as “an extremely dangerous approach to cryptographic design” with a myriad of critical vulnerabilities. Halderman Report, p. 29. For example, Section 6.1 of the Halderman Report states in relevant part that:

With access to the encryption and MAC keys from the Poll Worker Card, an attacker could decrypt or alter the ballot definitions used by the scanners and BMDs, forge ballot QR codes, or decrypt or modify election results on scanner memory cards before the results are returned to the EMS for reporting.

* * *

County election databases from the November 2020 and January 2021 elections shows that Georgia counties use the same cryptographic keys county-wide for each election. This means that if a single Poll Worker Card and PIN anywhere in a county is temporarily accessed by an attacker, the attacker can easily obtain the keys necessary to compromise election data throughout the county.

To make matters worse, if a county suspected that its keys had been compromised, the only way to change them would be to load new election definitions into every ICX and ICP in the county. Doing so would likely take days or longer and might necessitate repeating logic and accuracy testing on every device.

There (sic) problems are the result of an extremely dangerous approach to cryptographic design.

Id.

³ See <https://www.scribd.com/document/653246915/Halderman-Report-on-Georgia-Election-Security-FINAL-REPORT>(last visited Aug. 26, 2024).

Professor Halderman stated further at Section 9.1 that:

Moreover, all scanners and BMDs within each county use the same encryption key and initialization vector (IV) during a particular election. Given access to the county EMS or Election Package, the key and IV can be retrieved from the election project database using the SQL command:

```
SELECT RijndaelKey, RijndaelVector from
ElectionEvent;
```

I show in Section 6.1 that the same key and IV can also be extracted from any Poll Worker Card in the county, given brief access to the card and PIN. After obtaining the key and IV, the ICX election definition file can be decrypted using the following shell command:

```
openssl enc -d -aes-128-cbc -K $(xxd -pu <<<
'RijndaelKey') -iv $(xxd -pu <<< 'RijndaelVector')
-in ICX.dat -out ICX.zip.
```

Issue: *ICX election definition files are not digitally signed, and they can be modified by anyone with access to a symmetric encryption key that is shared by all scanners and BMDs within each county.*

Dominion could have used digital signatures to secure the ICX election definition files against malicious modification. Instead, there does not appear to be any cryptographic integrity protection, beyond verifying that the decrypted file is a properly formed Zip archive. As a result, anyone with access to the encryption key and IV discussed above can decrypt the ICX.dat file, modify it, and re-encrypt it using a command similar to the one shown above. My testing shows that the ICX will accept the modified file as if it were genuine.

Id. at pp. 48-49. (Italics in original). After reviewing the Halderman Report and the Dominion systems, on June 3, 2022, CISA eventually issued a bulletin recommending various corrections to security deficiencies but did not mention the failure to properly

store the encryption keys.⁴ Dominion later issued an updated version of its software to address the CISA bulletin's recommendations, but that updated version did not secure the encryption keys as required by EAC-certification requirements.

26.

While discussing encryption keys and their insecure storage, the Halderman Report made no reference to encryption modules or to the EAC certification requirements adopting the FIPS 140-2 standard for their storage.

27.

CISA has stayed silent about the insecure storage of encryption keys despite being put on notice of this security failure by Professor Halderman and despite election systems having been designated as Critical Infrastructure by the Secretary of the Department of Homeland Security. Likewise, Dominion has not addressed its failure to properly store the encryption keys.

28.

The Secretary of State has taken no action to remedy any of the deficiencies identified in either the Halderman Report or the CISA bulletin. Nor, in particular, has

⁴ See *Vulnerabilities Affecting Dominion Voting Systems ImageCast X*, CISA ICS Advisory, June 3, 2022, available at <https://www.cisa.gov/news-events/ics-advisories/icsa-22-154-01> (last visited Aug. 26, 2024).

the Secretary of State done anything to implement certification-compliant storage and management of the encryption keys on the Dominion system.

29.

The Secretary of State's General Counsel was notified by one of the undersigned counsel in March 2024 that the encryption keys are stored unprotected on county election databases and in plain text as alleged herein, and the State has not denied it.⁵ Moreover, the Secretary of State has had the Halderman Report identifying the insecure storage of the encryption keys since it was issued in July 2021. Nor has the State denied that, in this regard, the Dominion system is in material breach of the applicable EAC certification standards required by Georgia law.

30.

The VVSG system performance guidelines with which the Dominion system must comply require that certain specific categories of risk be addressed, including:

- Unauthorized changes to system capabilities for:
 - Defining ballot formats
 - Casting and recording votes

⁵ See Exh. 5, March 28, 2024 email correspondence between Kurt Olsen and Charlene McGowan, Counsel to the Secretary of State; and (2) Matt Naham, *Kari Lake to SCOTUS: Hurry up, the 2024 election is coming and Dominion voting machines need to be banned*, LAW AND CRIME, March 21, 2024, available at <https://lawandcrime.com/supreme-court/kari-lake-to-scotus-hurry-up-the-2024-election-is-coming-and-dominion-voting-machines-need-to-be-banned/> (last visited Aug. 25, 2024 (containing Dominion's response on the encryption keys issue)).

- Calculating vote totals consistent with defined ballot formats
- Reporting vote totals
- Alteration of voting system audit trails
- Changing, or preventing the recording of, a vote
- Introducing data for a vote not cast by a registered voter
- Changing calculated vote totals
- Preventing access to vote data--including individual votes and vote totals--by unauthorized individuals
- Preventing access to voter identification data and data for votes cast by the voter such that an individual can determine the content of specific votes.

VVSG Section 7 Security Requirements, 7.1 Scope, p. 124. The circumstances described herein constitute a comprehensive failure to secure Georgia's voting systems in these respects as required by the VVSG. Any malicious actor with remote or onsite access, exploiting availability of the encryption keys in plain text, can change information and election results in any of these categories without likely detection.

31.

The State's election systems do not comply with the requirements of the Help America Vote Act ("HAVA") or its related and integrated federal statutory requirements.

COUNT ONE – MANDAMUS ABSOLUTE

32.

The allegations of the foregoing paragraphs are realleged and incorporated herein by reference.

33.

The circumstances described herein present a grave and urgent cyber security risk to the integrity of Georgia elections and warrant expeditious mandamus relief to safeguard Georgia's elections.

34.

Pursuant to O.C.G.A. § 9-6-20 et seq., Applicant requests that the Court issue a writ of mandamus as soon as practicable to take evidence and consider the arguments of counsel, and enter a mandamus absolute ordering the Defendant to immediately bring the Dominion systems used in Georgia elections into compliance with Georgia law as aforesaid and as to be shown at any hearing on this matter.

35.

Applicant is entitled to a mandamus absolute, as a matter of law, ordering the Secretary of State of cause all encryption keys to be properly stored in an encrypted module as required by State law, the VVSG guidelines and FIPS 140-2, and to require all Counties to implement password and data retention and auditability practices that conform to the VVSG guidelines as set forth at Sections 2.1.5 System Audit; 2.1.5.1

Operational Requirements; 2.1.10 Data Retention; 5.3 Data and Document Retention; 5.4 Audit Record Data; 5.4.4 Vote Tally Data; 6.1.3 Data Transmission; 7.7.1 Controlling Usage [of Wireless Communications]; 7.9.3 Electronic and Paper Record Structure; 7.9.4. Equipment Security and Reliability.

36.

As a result of the foregoing, Georgia's election systems have been placed in an illegal and insecure state since at least 2020. Thus, Georgia's election systems may have already been compromised by malicious actors. O.C.G.A. § 9-6-21(a) provides that mandamus relief "shall not be confined to the enforcement of mere ministerial duties." In addition, the Secretary of State's ongoing failure to cause Georgia's election system to comply with the requirements of Georgia law as aforesaid constitutes a gross abuse of discretion. Accordingly, Applicant is entitled to the following further and additional interim or mitigating mandamus relief: namely that, consistent with the VVSG data and auditability requirements identified in paragraph 38 the Court order that all system logs, Cast Vote Records and ballot images be preserved and stored on read-only media and be made available to Applicant and the public for copying, downloading and/or inspection beginning within 24 hours of the close of the polls, continuing every 24 hours for any additional logs, records and reports produced thereafter, until the election has been certified. In addition, all system log files discussed above must be preserved and archived daily beginning with the first day that any ballot is cast on a ballot marking

device or scanned on a tabulator and made available on the same terms as requested above.

37.

Applicant also requests that Georgia State Election Board Rule 183-1-12-.12 *Tabulating Results* be followed as part of the Court's mandated relief.

38.

"Where the question is one of public right and the object is to procure the enforcement of a public duty, no legal or special interest need be shown, but it shall be sufficient that an Applicant is interested in having the laws executed and the duty in question enforced." O.C.G.A. § 9-6-24.

39.

The security of the State's elections is a question of public right. The Secretary of State has a ministerial duty to comply with O.C.G.A. § 21-2-300(a)(2) and (3) and to require compliance with the VVSG standards that require use of a secure encrypted module for storage of encryption keys and proper password management. These duties affect the people at large rather than only Applicant. *Adams v. Ga. Dep't of Corr.*, 274 Ga. 461, 462 (2001) (stating that a public duty is "one which affects the general public rather than a private individual").

40.

The Defendant has failed to comply with the Georgia Election Code and other mandatory regulations that govern the secure administration of our State's elections as described herein.

41.

The Defendant is the official required by law to perform the specified acts, *see City of Lawrenceville v. Humphries*, 229 Ga. 724, 726 (1972), yet the Defendant has refused to properly secure the State's elections, as required by law as described herein.

42.

The Applicant has no other adequate and specific legal remedy for the Defendants' failure as described herein to properly secure the State's elections, as required by law.

43.

The Secretary of State is the proper defendant for the writ of mandamus sought herein because (1) the Secretary of State requires the counties to use the Dominion system, (2) the Secretary of State purchased and furnished the Dominion system to each of the various counties, (3) State law and the Secretary of State specify by state statute and state regulation or other less formal administrative guidance nearly every aspect of how the Dominion system is to be stored, installed, tested, and operated, (4) the Secretary of State has the requisite authority and a ministerial duty to enforce the

requirements of state law that are referred to herein and to effectuate the relief sought herein, and (5) the counties, on the other hand, do not have sufficient authority or control over the certification, configuration or operation of the Dominion systems to make the changes necessary to cause Georgia's election computer systems to comply with State law or to otherwise mitigate the security risks identified herein or otherwise to effectuate the relief sought herein.

44.

In addition, any remedial measures must be applied state-wide in a uniform fashion in order to ensure that all Georgia voters are voting on a level playing field in order to comply with state law requiring such uniformity and with the Equal Protection Clause of the U.S. Constitution. It is the duty of the Secretary of State to ensure such uniformity and thus the Secretary of State is the proper party defendant for the relief sought in this case.

45.

Applicant is entitled to a mandamus absolute as prayed herein in order to ensure that the State's elections are secure and the rights of the State's voters and candidates and its' members are secured in accordance with the state election code.

46.

A post-election challenge to the results of the election based on the cyber security vulnerabilities alleged herein is not an adequate remedy at law because the remedy

sought herein, namely an order compelling the Secretary of State to bring Georgia's election systems into compliance with State law, is not available in an election contest under O.C.G.A. § 21-2-520 et seq.

47.

In addition, any post-election suit seeking the relief sought herein might be barred by the doctrine of laches on the grounds that it could have and should have been raised sooner.

48.

In addition, an election contest under O.C.G.A. § 21-2-520 et seq. based on the cyber security vulnerabilities alleged herein, which must be filed within five days of certification, might be infeasible or impossible due to the extreme difficulty, within the severely limited time available, of gathering, analyzing, detecting and presenting evidence of any fraud or irregularity made possible by exploiting such vulnerabilities.

49.

Lastly, fixing these problems after the election would not afford effective relief for the 2024 election for the same reason that closing the barn door after the horse has left is not an effective remedy against the risk that the horse might get away. As to future elections after 2024, relief should be ordered sufficiently in advance to be effective in those elections.

50.

This is especially true because the failure of the State to properly secure elections might be exploited by sophisticated malicious actors that would leave no detectable trace.

PRAYER FOR RELIEF

51.

Wherefore, Applicant respectfully prays,

- (a) that process issue and be served with the Application upon the Defendant;
- (b) that the Court expeditiously issues a mandamus nisi to consider the issuance of a mandamus absolute;
- (c) that the Court conducts an evidentiary hearing to consider the issuance of a mandamus absolute;
- (d) that the Court issues a mandamus absolute to order the Secretary of State of Georgia to comply with the aforementioned Georgia elections code and other elections regulations;
- (e) that the Court grant the further and additional interim mitigating relief as prayed herein.
- (e) for such other and further relief as to the Court seems proper and just.

Respectfully submitted, this 29th day of August, 2024.

**CALDWELL, CARLSON, ELLIOTT &
DELOACH, LLP**

/s/ Harry W. MacDougald
Harry W. MacDougald
Ga. Bar No. 463076
6 Concourse Parkway
Suite 2400
Atlanta, Georgia 30328
(404) 843-1956
hmacdougald@ccedlaw.com

OLSEN LAW, P.C.

Kurt B. Olsen*
1250 Connecticut Ave., NW, Ste. 700
Washington DC 20036
(202) 408-7025
ko@olsenlawpc.com

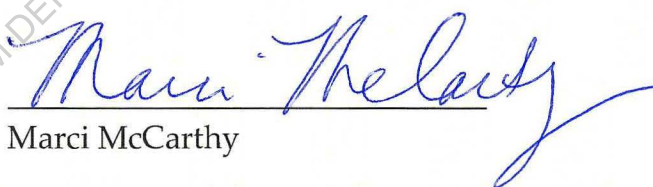
* *Pro Hac Vice Application forthcoming*

HARDING LAW FIRM, LLC

/s/ Todd A. Harding
Todd A. Harding, For the Firm
Ga. Bar No.: 101562
Attorney at Law
HARDING LAW FIRM, LLC
113 E. Solomon Street
Griffin, Georgia 30223
(770) 229-4578
(770) 228-9111 facsimile

VERIFICATION

Marci McCarthy, being first duly sworn on oath, deposes and says that she is the Chair of the DeKalb County Republican Party, Inc., the Applicant in this matter, that she has read the foregoing Application for a Writ of Mandamus and knows the contents thereof, that said Application was prepared with the assistance and advice of counsel and the assistance of expert witnesses upon which she has relied; that the allegations set forth herein regarding the DeKalb County Republican Party, Inc. are true and correct to the best of her knowledge, information and belief, and that she has relied on the expert witness affidavits filed herewith with respect to the matters set forth therein.



Marci McCarthy

Sworn to and subscribed before me
this 29th day of August,
2024.



Notary Public
My Commission Expires: 5/7/28





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

Contract No. [●]

RETRIEVED FROM DEMOCRACYDOCKET.COM

Master Solution Purchase and Services Agreement

THIS MASTER SOLUTION PURCHASE AND SERVICES AGREEMENT (this “**Agreement**”) is entered into this ____ day of _____, 2019 (the “**Effective Date**”), by and between the Secretary of State of the State of Georgia, with its principal executive offices at 2 Martin Luther King Jr. Drive, West Tower, Atlanta, Georgia 30334 (“**State**”), and Dominion Voting Systems, Inc., with an office at 1201 18th Street, Suite 210, Denver, Colorado 80202 (“**Contractor**”). All capitalized terms used in this Agreement are defined, or the location of such definitions indexed, in Section 18.

1. BACKGROUND AND SCOPE.

1.1 **Background.** State desires to acquire, and enable other State Entities to acquire, from Contractor certain Services, Software, Equipment and/or any Licensed Programs or any combination of the foregoing (collectively, the “**Solution**”) capable of providing a new Statewide Voting System (a “**SVS**”) with a verifiable paper record which is sufficient to support all primaries and general elections, as more fully described in State’s request for proposal for the Solution (event number 47800-SOS0000037) released March 15, 2019 and all documents attached thereto or links contained therein (as amended, the “**eRFP**”). Based on Contractor’s experience, State has selected Contractor to supply such Solution and, if selected by State, to perform (through itself or one or more Contractor Solution Partners) Services to customize, install, implement and/or maintain a Solution, as further described herein.

1.2 **Guaranteed Functionality & Guaranteed Performance.** Before the selection of Contractor, State issued the eRFP whereby Contractor was required to make an initial, written response to such eRFP and to engage in meetings and discussions with State regarding the suitability of the Solution and Services for identified needs of the State Entities as set forth in the eRFP. As part of the eRFP process, State required Contractor to perform certain professional services and demonstrations to validate and confirm that the Solution and Services fulfill the needs of the State as described in the eRFP, including the delivery and implementation of a SVS that can be used by all State Entities throughout the State of Georgia for the 2020 Presidential Preference Primary on March 24, 2020 (the “**Presidential Preference Primary**”). Such requirements, together with Contractor’s eRFP Response, Contractor’s Request for Supplemental Technical Response dated June 24, 2019, shall be considered the “**Mandatory Requirements**” for purposes of this Agreement, which shall be incorporated in writing into this Agreement. Contractor expressly represents that the Solution will meet all Mandatory Requirements, and, when implemented, will accurately function in accordance with those requirements and this Agreement. State selected Contractor and the Solution and enters into this Agreement based on the features, functions and attributes of the Solution described in (a) the Documentation, (b) the Mandatory Requirements as being capable of enabling State and all other State Entities to accurately and securely administer elections throughout the State of Georgia in accordance with Applicable Laws of the State of Georgia (the “**Guaranteed Functionality**”), and (c) Contractor’s guarantee that Contractor will have timely and completely implemented the Solution prior to the date of the Presidential Preference Primary (March 24, 2020), including delivery of all Equipment and training on the use of such Equipment in the registration of voters and administration of an election, such that the SVS is in place and the Solution fully operational and available for use by all State Entities in such Primary and in all subsequent primary and general elections throughout the Term (the “**Guaranteed Performance**”).

1.3 **Solution Partners.** Contractor may provide certain of the Services and/or components of the Solution (including certain Third Party Licensed Programs) through one or more Contractor Affiliates, suppliers, resellers, or service providers (each, a “**Contractor Solution Partner**”), provided, each is expressly identified by Contractor to State and State agrees to its inclusion on Exhibit D hereto. As between Contractor and each Contractor Solution Partner on the one hand, and State on the other hand, Contractor shall be the prime contractor to State hereunder and in such capacity shall have full responsibility and liability for the performance of the Solution (including each of its Contractor Solution Partner components) and all Services hereunder (including all Services provided by Contractor Solution Partners). Unless the context otherwise requires, all references to “**Contractor**” throughout this Agreement shall refer to both Contractor and each Contractor Solution Partner. If any Services or any portion or component of the Solution is subject to a warranty claim or otherwise suffers a malfunction or defect and Contractor and a

Contractor Solution Partner dispute the cause of and/or fault for such malfunction or defect, then until such time as Contractor and the Contractor Solution Partner resolve their dispute, Contractor shall, without delay or cost to State continue to provide the Maintenance Services and complete all repairs, replacements or other applicable remedy obligations hereunder as necessary to full remedy the warranty claim.

1.4 Purchasing by State and other State Entities. State may use the Solution and/or Services purchased under this Agreement on its own behalf and for the benefit of all other State Entities, in accordance with the terms and conditions hereof. Contractor acknowledges and agrees that this Agreement is intended to be subject to an intergovernmental agreement between State and the other State Entities, and, therefore, that State or any other State Entity may purchase the Solution and/or any of the Services directly under this Agreement by issuing a valid purchase order and entering into a Solution Order or Services Order, as applicable. Any State Entity directly purchasing a Solution and/or Services under this Agreement (i) shall be solely responsible for payment of the Solution or Services purchased by such State Entity, (ii) shall be entitled to all of the rights and benefits afforded to State under this Agreement, and (iii) may enforce this Agreement in its own name with respect to such Solution and/or Services as if this Agreement, in its entirety, had been executed by Contractor and the applicable State Entity, and (iv) subject to Section 17.6.1, shall only be held responsible by Contractor for the performance of its obligations (including payment obligations) with respect to the specific Solution and/or Services purchased by such State Entity as set forth in the applicable Solution Order or Services Order.

1.5 Non-Exclusive Rights. This Agreement is not exclusive. State and each other State Entity reserve the right to select other contractors to provide the same or other products, licenses and services.

1.6 No Minimums Guaranteed. Except as provided in an executed Solution Order, this Agreement does not guarantee any minimum level of purchases.

2. SOLUTION AND DELIVERABLES.

2.1 Solution Order and Delivery. During the Term, and subject to all of the terms and conditions contained herein, Contractor agrees to deliver to State the Solutions ordered pursuant to a Solution Order, as hereinafter described.

2.1.1 Solution Order. For the ordering of a Solution from Contractor, any State Entity and Contractor will, subject to mutual agreement by both parties, execute a written order (each an "**Solution Order**"). Each Solution Order shall: (a) be substantially in the form of Exhibit B hereto; (b) be consecutively numbered with respect to all prior Solution Orders; and (c) include, where applicable and available at that time, the following information:

(i) the services described in this Agreement, including the Configuration Services, services required to complete Installation Events, Maintenance Services, Training Services and other services provided by Contractor under this Agreement (the "**Services**"), which are being purchased by the applicable State Entity;

(ii) licenses and/or sublicenses to the application software (the "**Application Programs**"), and to the custom programming application software (the "**Special Programs**") required in connection with the Services;

(iii) the software support services to be provided by Contractor for the Application Programs and the Special Programs (collectively, the "**Support Services**");

(iv) the hardware and equipment Deliverables to be provided by Contractor hereunder, including any computer systems, accessories, supplies, parts, related Documentation, and Revisions thereto to be provided by Contractor required for the operation of the Solution (the "**Equipment**") and the licenses and/or sublicenses to the operating software for such Equipment granted by Contractor (the "**Operating Programs**");

- (v) the maintenance services for the Equipment (collectively, the “**Maintenance Services**”);
- (vi) the date by which the Solution must be fully delivered;
- (vii) the particular State Site to which such Solution must be delivered; and
- (viii) the price applicable to the items set forth on such Solution Order.

The terms “Application Programs,” “Special Programs,” and “Operating Programs” are collectively referred to as the “**Software**.” In the event of a conflict between the terms of this Agreement and the terms of any Solution Order, except with respect to any provision of this Agreement which explicitly states that it may be modified or superseded by an analogous provision in a Solution Order, the terms of this Agreement shall control. The terms and conditions of each Solution Order will apply solely with respect to the Solution purchased under such Solution Order and shall not be deemed to modify this Agreement.

2.1.2 Implied Products and Services. Subject to Section 2.3.2 if any Services, Application Programs, customizations, Operating Programs, Support Services, Maintenance Services which are reasonably required for, and incidental to or inherent in, the proper delivery and use of the Solution or the performance and provision of the Services (regardless of whether they are specifically described in this Agreement), they will be deemed to be implied by and included within the scope of the Solution and Services to be provided by Contractor to the same extent and in the same manner as if specifically described in this Agreement.

2.1.3 Installation Plan. Attached as Attachment 4 to each Solution Order shall be an installation plan, developed by Contractor and approved by State (the “**Installation Plan**”) which describes in detail with respect to such Solution Order: (i) each element of the delivery, installation, and training of State Personnel in the operation and use of, the Solution, each in a manner that meets the Mandatory Requirements (each a “**Installation Event**”); (ii) the specific dates set by which each of the Installation Events are to be completed (the “**Installation Deadlines**”); and (iii) the applicable Site Specifications, if any. Installation Plans may be replaced and superseded from time to time upon agreement of the parties in order to reflect mutually agreed changes in the Installation Events or Installation Deadlines by using the change control procedures set forth in Section 5.2. For the avoidance of doubt, State Entities will only be responsible for those fees related to Installation Events that are reflected in the applicable Solution Order.

2.1.4 Delivery. Contractor shall deliver the Solution ordered, including all Equipment and Documentation, to the State Site specified in the Solution Order, by the date(s) specified in the Installation Plan and otherwise in strict compliance with the terms and conditions of this Agreement and Installation Plan. Contractor shall not make any substitutions for the Solution of any other version, model, capacity or manufacturer without the prior written consent of State. Contractor represents and warrants that the Solution shall be new (not remanufactured or refurbished), free of defects, and in good operating condition at all times prior to the expiration of the Warranty Period. Solutions which consist solely of Licensed Programs may also be delivered electronically upon mutual agreement of the parties.

2.1.5 Shipment, Title and Risk of Loss. For each piece of Equipment or other Solution hardware component, Contractor shall pass title and ownership of such Solution component to State upon State’s payment in full for such Solution component. Upon State’s payment in full for each Solution, Contractor will deliver a bill of sale for each Solution component to State, as applicable. Contractor guarantees that State shall acquire good and clear title to the Equipment and other Solution hardware components being purchased hereunder, free and clear of all liens and encumbrances. Contractor shall arrange for shipment, at Contractor’s expense, of Equipment by a mutually acceptable common carrier F.O.B. to the applicable State Site, or other delivery location specified in the Solution Order, at a mutually agreeable time. Risk of loss for such Equipment shall pass to State upon proper delivery at the designated destination. There shall be no additional charge to State for shipping, delivery or insurance beyond the prices set forth in the Solution Order. In the event of damage to any Equipment or hardware during transit or if Contractor or its designee delivers Equipment or hardware that does not pass Acceptance Testing, then Contractor will replace such

Equipment or hardware at Contractor's expense, including covering all shipping costs associated with returning such items to Contractor.

2.1.6 Inspection. In accordance with the Installation Plan and the requirements for the Acceptance Testing Plan, all Equipment shall be inspected as follows: (i) following arrival of the initial deliveries at the central warehouse designated by State and (ii) for the same deliveries, when forwarded to the State Site (or any subsequent delivery made directly to the State Site(s)). Prior payments shall not be considered as waiving any right of testing or inspection of the State Entities under this Agreement. Determination by a State Entity that Equipment or component has passed Acceptance Testing is without prejudice to any other rights or remedies that such State Entity may have with respect to any subsequently uncovered non-compliance, defect, or non-conformity. Any State Entity may return any Equipment or component of the Solution to Contractor that it determines not to have passed Initial Testing or Acceptance Testing for replacement, and such returns shall be at Contractor's expense including as relates to transportation charges. Any return made by a State Entity for failure of the Equipment or any component of the Solution to pass the Acceptance Testing shall not be affected by any determination by State that such Equipment or component passed Initial Acceptance Testing. If Contractor fails to repair or arrange shipment and pickup of such rejected Equipment by a mutually acceptable common carrier (F.O.B. the State Site from which such rejected items will be dispatched) and redeliver appropriate replacement Equipment or components sufficient to cure the defect prompting the rejection and otherwise fully functional in accordance with the requirements of this Agreement, within thirty (30) days of the applicable State Entity's notification of such rejection, the State Entity shall be entitled to, at its option: (a) rescind the applicable Solution Order as to the rejected Equipment; (b) accept the rejected Equipment or component at an equitable price reduction agreed by the parties; or (c) demand specific performance.

2.1.7 Cancellation of Solution Order for Convenience. A State Entity may cancel a Solution Order or any part thereof at any time without charge or cancellation fee. If State cancels any Solution Order, other than pursuant to Section 2.1.6, then the applicable State Entity will bear the cost of shipping any Equipment already delivered pursuant to such Solution Order back to location designated by Contractor (F.O.B. the State Site from which such rejected items will be dispatched). The remedy set forth in this Section 2.1.7 shall be Contractor's sole and exclusive remedy and State's entire liability for claims related to any such cancelled Solution Order. Where a Solution Order is terminated by a State Entity pursuant to this Section 2.1.7, State or the other State Entity, as applicable, shall pay to Contractor for the Equipment actually delivered and used by the applicable State Entity and the Services satisfactorily performed by Contractor, in each instance, prior to the date of such termination. If a State Entity has prepaid Contractor any amounts under a Solution Order terminated pursuant to this Section 2.1.7, Contractor will refund to the applicable State Entity that portion of such prepaid expense which is attributable to month(s) of and after the termination of the applicable Solution Order.

2.2 Documentation. Contractor shall deliver to State in such form as State shall request the number of copies requested by State of Documentation relating to the Solution and any updates thereto at no additional charge to State. State Entities may duplicate the Documentation provided that the State Entities reproduce the copyright that appears on such Documentation being duplicated. In no event will any provision of this Agreement, or any right or benefit of State or the other State Entities provided for under this Agreement, be reduced, limited or otherwise adversely affected (including through any increase in cost, charge or expense, including taxes) as a consequence of the terms of the Documentation.

2.3 Revisions; Upgraded Solution.

2.3.1 If Contractor makes any revision, modification, enhancement, improvement or otherwise updates the Software, any component thereof, or code used therein to include any patches, upgrades, updates, new versions, substitutions, replacements, and other modifications, improvements and enhancements, including through the introduction of new products that have comparable purpose and functionality as the Software used by the State Entities (collectively the "**Revisions**"), such Revisions will be made available to the State Entities, and, if approved by State, provided by Contractor, on a no-charge basis (with a corresponding credit for the amortized cost of the component being replaced by the accepted Revision) and will be deemed to be part of the Solution. Contractor shall keep State informed of any

potential Revisions being considered by Contractor, Revisions which may be necessary to keep the Solution relevant, and any developments in the industry or election practices generally that could adversely affect the Solution or render it obsolete including by: (i) meeting with State quarterly throughout the twenty-four (24) months immediately following the Effective Date and then twice in each of the successive twelve (12) month period remaining during the Term to discuss the same and (ii) providing State with a detailed comparison of the Solution currently in use by the State Entities as of the date of the Proposed Revisions as would exist after any proposed Revisions (the “**Upgraded Solution**”). The Upgraded Solution and the Revisions contained therein shall be subject to State’s prior review and approval and State may conduct such testing and evaluations of the same as it determines to be necessary. If State declines to use the Revisions or the Upgraded Solution, Contractor will remain obligated to support the existing version of the Solution during the Term. For the avoidance of doubt, except as otherwise specified in Section 2.3.2, Contractor shall provide all Revisions occurring at any time during the Term at no additional cost to, and without increases to any existing fees payable hereunder by, any State Entity.

2.3.2 If a State Entity requests that Contractor make Revisions to the Software that are major in nature and are required because of a change to Applicable Laws of the State of Georgia governing elections as in effect as of the date of this Agreement (e.g. a change to a ranked-choice voting system) (“**Major Revisions**”) such Major Revisions may be accompanied by additional or increased fees as mutually agreed upon by the parties in accordance with the Change Request procedure described in Section 5.4. Notwithstanding the foregoing, Contractor acknowledges and agrees that any Revisions or other changes to the Solution that are required due to changes in federal law, regulation, or standard shall not be accompanied by an increased fee.

2.3.3 Throughout the Term and subject to any restrictions on implementing changes or adding services under this Agreement, Contractor will seek to improve the quality, efficiency and effectiveness of the Solution to keep pace with technological advances and support State’s evolving needs as related to election administration. Without limiting the generality of the foregoing, Contractor will: (a) identify and apply ‘best practice’ techniques and methodologies in performing and delivering the Solution and Services consistent with then-current industry standards and Contractor’s normal course of business; (b) train Contractor Personnel in new techniques and technologies used generally within the industry; and (c) maintain the currency of the Contractor’s tools, infrastructure, software and other resources. Notwithstanding anything contained herein to the contrary, Contractor shall not, without the prior written consent of State, (i) make any Revision or otherwise add to or alter the Solution or any component part thereof in any way that could remove Guaranteed Functionality or materially degrade Guaranteed Performance (or any portion thereof) or (ii) fail to make any Revisions necessary to ensure the Solution used by the State Entities remains current and at the forefront of voting technology throughout the Term, provided that such Revisions have been certified under the applicable provisions of the election laws and regulations of the State of Georgia, to the extent such certification is required.

2.4 Additional Requirements and Dependencies. Items or services which are included in or required for a Solution but not provided directly by Contractor must be identified as such in the Schedule for the corresponding Solution. Items or services which are required but are not available without further development or engineering must be identified as such in the Schedule for the corresponding Solution. If for any Solution Contractor sells or licenses to State Contractor’s own or a Contractor Solution Partner’s software, hardware, network communications, or interfaces, including project tools that Contractor regards as proprietary, Contractor will provide State, in addition to descriptions contained in a Schedule, a separate purchase order, contract, or license agreement describing the terms of such transaction. State will not be subject to extraneous royalties or other extended payment terms or usage restrictions of any kind arising from the purchase or license of such items unless shown in such purchase order, contract, or license agreement and unless such purchase order, contract, or license agreement is approved in writing by an authorized representative of State.

2.5 Within industry standards, State reserves the right to select the features, tools, accessories and companion applications to be used with the Solution to the extent reasonably necessary for the administration of elections. Contractor agrees to work with the other contractors who offer such products

and solutions. State reserves the right to approve system configuration, architecture, or functionality that affects the choice or use of the third-party products.

3. LICENSE AND AUTHORIZED USE.

3.1 Grant of License.

3.1.1 **Grant of License.** Except as provided elsewhere in this Agreement or an applicable Solution Order, Contractor hereby grants to State a non-exclusive, irrevocable (during the Term), and worldwide license for State and other State Entities to use, install, execute, store, and display the object version of all Contractor Licensed Programs in connection with State's use, operation, or support of the Solution and in accordance with all the terms and conditions of this Agreement. In addition, State, the other State Entities, and/or State Contractors, subject to the restrictions and processes set forth herein, shall be permitted, in connection with the use, operation, or support of the Solution, to: (a) use the Contractor Licensed Programs at any State Site; (b) make and use copies of the Contractor Licensed Programs at each State Site; (c) use the Contractor Licensed Programs for to fulfill the Mandatory Requirements including by providing access at all applicable State Sites to the Contractor Licensed Programs, other than by remote connection; and (d) use and/or copy of the Contractor Licensed Programs for the purpose of creating and using training materials relating to the Contractor Licensed Programs for internal purposes, which training materials may include flow diagrams, system operation schematics, or screen prints from operation of the Contractor Licensed Programs.

3.1.2 **License to Source Code Version.** The License also includes the right to receive from Contractor and use the source code version of the Contractor Licensed Programs to the extent so provided in Section 3.1.4 and Section 3.2.

3.1.3 **Deactivation at State's Request.** From time to time, a State Entity may elect to uninstall one or more Contractor Licensed Programs for some period of time. If a State Entity elects to uninstall any Contractor Licensed Program such State Entity shall not be responsible for payment of any further fee applicable to such uninstalled Contractor Licensed Program(s). If a State Entity elects to reinstall any such Contractor Licensed Program(s) (i) the Extended Warranty applicable to such Contractor Licensed Program(s) will recommence as of the date such Contractor Licensed Program(s) is reinstalled and (ii) any such reinstallation by a State Entity will be at no cost to any State Entity other than as provided above.

3.1.4 **Rights Upon Contractor Insolvency.** All rights and licenses granted under or pursuant to this Agreement by Contractor to State and any State Entities are, and shall otherwise be deemed to be, for purposes of Section 365 (n) of the United States Bankruptcy Code ("**Bankruptcy Code**"), licenses to rights to "intellectual property" as defined under the Bankruptcy Code. Contractor acknowledges that if it, as a debtor in possession or a trustee in bankruptcy in a case under the Bankruptcy Code, rejects this Agreement, then State or a State Entity may elect to retain its rights under this Agreement as provided in Section 365(n) of the Bankruptcy Code. The parties further agree that, in the event of the commencement of any bankruptcy proceeding by or against Contractor under the Bankruptcy Code, State and each State Entity shall be entitled to retain all of such rights under this Agreement. Contractor agrees and acknowledges that enforcement by State or any State Entity of any rights under Section 365(n) of the Bankruptcy Code in connection with this Agreement shall not violate the automatic stay of Section 362 of the Bankruptcy Code and waives any right to object on such basis. Upon rejection of this Agreement by Contractor or the bankruptcy trustee in a bankruptcy case under the Bankruptcy Code and written request of State or a State Entity to Contractor or the bankruptcy trustee pursuant to Section 365(n) of the Bankruptcy Code, Contractor or such bankruptcy trustee shall: (a) provide State or such State Entity the materials that are the subject of the rights and licenses described in this Section 3.1.4 and any Intellectual Property Rights otherwise required to be provided to State or such State Entity under this Agreement, or any agreement supplementary to this Agreement, held by Contractor or such bankruptcy trustee; and (b) not interfere with the rights of State or such State Entity provided in this Agreement or any other agreement supplementary to this Agreement, to the materials that are the subject of the rights and licenses described in this Section 3.1.4, and any Intellectual Property Rights provided under such agreements, including any

right to obtain the materials that are the subject of the rights and licenses described in this Section 3.1.4 and any such Intellectual Property Rights from another party.

3.2 Delivery and Use of Source Code. No later than thirty calendar days from State of Georgia certification, Contractor shall, at its sole expense, (i) place in escrow with NCC Group, Inc., a Virginia corporation (the "**Escrow Agent**"), pursuant to the NCC Group Sourceone Escrow Agreement (Agreement# 46286) by and between Escrow Agent and Contractor dated November 4, 2010 (the "**Escrow Agreement**"), a copy of the Source Code incorporated within the Solution provided to the State Entities under this Agreement and (ii) cause the State to be enrolled as a "Licensee" under the Escrow Agreement. Delivery of such Contractor Licensed Programs under this Agreement will be deemed to include and require delivery of a copy of the Source Code to the Escrow Agent under the Escrow Agreement, together with any updates thereto. State shall be entitled to receive a copy of such Source Code and to use such Source Code to support and maintain the State Entities' authorized use of the Contractor Licensed Programs, upon the occurrence of a "Release Event" set forth in the Escrow Agreement. If Contractor makes any update to any escrowed Contractor Licensed Program, Contractor shall furnish the Escrow Agent with a corrected or revised copy of the Source Code for such Contractor Licensed Program within the timeframe required by Section 1.2 of the Escrow Agreement.

3.3 Third Party Source Code. Contractor shall identify to State in writing prior to the Effective Date and from time to time thereafter as often as required, any source code for Third Party Licensed Programs that Contractor is not authorized to deliver as part of the Source Code hereunder and for all such source code.

4. Services.

4.1 Configuration Services.

4.1.1 State Solution and Functional Requirements. Contractor acknowledges that State has relied, and will rely on, Contractor's experience and expertise in installing, implementing, and servicing the Solution purchased under this Agreement. The Solution will, when installed and implemented, meet State's technology and business requirements including all Functional Requirements. For purposes of this Agreement "**Functional Requirements**" means the technical requirements of State including, where applicable: (a) an identification of all software applications to be run on such Solution (including Licensed Programs provided by Contractor under this Agreement) (collectively, the "**Designated Licensed Programs**"); (b) any performance requirements of the Solution, as applicable (the "**Performance Requirements**"); (c) the anticipated number of users of the Solution and/or Designated Licensed Programs; and (d) details relating to any State systems with which the Solution and Designated Licensed Programs are to interface. Any Functional Requirements described in the Installation Plan, Solution Order, or Services Order shall be incorporated herein.

4.1.2 Contractor System Proposal. If State provides Contractor with Functional Requirements, Contractor shall, at no additional cost to State, analyze such Functional Requirements to determine the minimal amount and type of Solution that Contractor believes State needs to purchase in order to meet the Functional Requirements. Within ten (10) business days of its receipt of the Functional Requirements, Contractor shall deliver to State a written proposal (each a "**Contractor System Proposal**") which shall thereupon become part of the Guaranteed Functionality and be attached to the applicable Solution Order. The Contractor System Proposal shall detail at a minimum (as applicable): (a) the Solution components required to meet the applicable Functional Requirements; (b) the minimal operating system, network, and third-party software necessary to run the Designated Licensed Programs in conformity with the Functional Requirements; and (c) the estimated cost for such Solution determined in accordance with this Agreement. Nothing contained in the Contractor System Proposal shall obligate State to purchase any Solution or portion thereof.

4.1.3 Attachments to Solution. Subject to the other terms of this Section, in the event State provides Contractor with Functional Requirements for a certain Solution (and obtains confirmation of approval thereof as required below), State shall be entitled to install any attachment, feature, or device to, or install any Licensed Programs, on such Solution without affecting Contractor's representations and

warranties hereunder, if within a reasonable period of time not to exceed thirty (30) business days after receipt from State of notice of its intent to do so (such notice to be addressed to the Contractor Relationship Manager and delivered via return receipt mail), Contractor provides written notice to State either confirming compatibility with the Solution of the such items or stating reasonable grounds upon which it concludes such attachment, feature, device, modification, change, enhancement, upgrade, or addition will adversely affect its obligations, including any warranty or representation hereunder. Contractor shall use reasonable efforts to respond to any such request. Any request for such confirmation from State as provided under this Section that is not responded to by Contractor shall be deemed an acceptance by Contractor of the compatibility of such items with the Solution. If after receipt of the Contractor notice advising State of Contractor's conclusion that such attachments, features, or devices will adversely affect its obligations State employs such attachment, feature, device, modification, change, enhancement, upgrade, or addition, Contractor shall not be liable for those representations and warranties that it notified State it reasonably concluded would be adversely affected as identified in the detailed notice.

4.2 Extended Warranty. Contractor shall provide from the Effective Date until December 31, 2021 and thereafter for so long as requested by each State Entity, a "total care solution" for the Solution, which, in addition to basic commitments contained in this Agreement, will include service guarantees sufficient to keep the Solution in good operating order in accordance with the Mandatory Requirements at all times (the "**Extended Warranty**"). The Extended Warranty will include all Maintenance Services, telephone and online support, installation assistance, troubleshooting, "break-and-fix," replacement or repair of Equipment and components. Contractor will, at its own expense, upon receipt of written notice from a State Entity of an Extended Warranty claim make all adjustments and modifications necessary to cure any defect or nonconformity affecting the Solution such that it is fully functional in conformity with the specifications and requirement set forth herein. Contractor shall immediately commence correction of all Extended Warranty claims made pursuant to this Section 4.2. For the avoidance of doubt, the parties acknowledge and agree that no fees, charge, or other costs associated with maintenance, repair, modification, adjustment, replacement, or other remediation of the Solution will be owed by any State Entity in connection with the Extended Warranty. The Extended Warranty shall be "all inclusive." If the parties agree that State or any of its personnel shall perform any services relating to an Extended Warranty claim on behalf of Contractor, State shall receive a credit against the next Milestone Payment to the extent of the services so performed by State. Notwithstanding the administration of any services by a State Entity on behalf of Contractor in connection with the maintenance or support of the Solution, Contractor shall at all times be responsible the integrity and quality of all Services and the Solution. Without limiting the foregoing, the following conditions apply to the Extended Warranty:

4.2.1 State Entity shall bear the shipping costs to return the malfunctioning item of Hardware to Contractor, and Contractor shall bear the costs for ground shipping the repaired or replaced item of hardware to State Entity. Shipping costs are based on ground service rates. If faster shipping service is required, the shipping cost shall be at the State Entity's expense.

4.2.2 Repairs will be conducted and parts replaced at the Contractor repair depot, followed by an inspection.

4.2.3 The following services are among those not covered by this Warranty, but will be made available to the State Entities at Contractor's time and material rates specified on the Fee Schedule:

- (a) Replacement of the following consumable items required for operation of the Equipment: batteries, paper rolls, ribbons, seals, smart cards, and removable memory devices and disks;
- (b) Replacement of Equipment that has been irreparably damaged by abuse by acts of the State or its employees;
- (c) Replacement of Equipment that is lost due to theft;
- (d) Repair or replacement of hardware damaged by of accident, disaster, theft, vandalism, neglect, or abuse;

(e) Repair or replacement of hardware Equipment that has modified by any Person other than those expressly authorized in writing by Contractor; and

(f) Repair or replacement of Equipment from which the serial numbers have been removed.

4.3 Training Services. Contractor shall provide training services ("**Training Services**"), for the fees set forth in the Solution Order, on such dates and locations mutually agreed upon, and shall make available any additional training requested by State which will be for the fees set forth in an additional Services Order Attachment (defined below). In addition and at no cost to State, upon request by State, Contractor shall (a) prior to the date of the Presidential Preference Primary provide (March 24, 2020) up to ten (10) business days (consecutive but for intervening weekend) of training to up to four (4) State designated personnel covering basic level 1 support issues relating to the maintenance of such initial Solution, and (b) up to three (3) business days (consecutive) of training for to up to four (4) State designated personnel on similar issues during each subsequent period. All such training shall occur at the Contractor designated Contractor location within Georgia, and State shall be responsible for all travel, living and other out-of-pocket expenses incurred by such State designated personnel to attend such training. State shall have the right, at its expense, to copy and distribute any and all training materials within State and its other State Entities, and to distribute such materials to train its personnel in the use of the Solution without additional charge by Contractor, provided all proprietary notices of Contractor are duplicated and no modifications to such materials are made without Contractor's prior written consent. Contractor represents that the Training Services described in the Training Plan attached to the Solution Order as Attachment 6 are designed to enable State personnel to productively use and operate the Solution. All Training Services shall be conducted by qualified instructors.

4.4 Other Services. In the event State wishes Contractor to provide software development or software customization, and/or consulting services, such Services shall be provided pursuant to written Services Orders detailing the Services to be performed. Each such Services Order shall have attached to and incorporated into it all delivery, Milestone Schedules, Specifications, Performance Levels (or other Service Level Agreements), disaster recovery plans or other mutually agreed project requirements or documents related to the Services to be provided (each a "**Services Order Attachment**"). All Services Orders and Services Order Attachments shall be mutually agreed by the parties and executed by their authorized representatives but shall take substantially the form contained in Exhibit C to this Agreement. All Services Orders require a validly issued State purchase order. Notwithstanding anything contained in this Agreement to the contrary, all Services ordered by a State Entity, and provided by Contractor, pursuant to a Services Order shall be included with the annual License Fee set forth on the Fee Schedule payable by the State Entities, except where such Services are required because of a Major Revision, in which case additional fees may be agreed upon by State and the Contractor in accordance with Section 2.3.2.

5. CHANGE CONTROL.

5.1 No Deviation. Contractor shall not deviate from the terms and conditions of a Solution Order or Services Order by substitution, deletion, or additions to the Solution, Services or other Deliverables without prior written approval or consent to waiver signed by a duly authorized representative of State or the applicable State Entity. Either party may request or recommend changes by following the change control procedures set forth in this Section 5.

5.2 Change Order. Either party may request or recommend changes to the Solution, Services or the scope or nature of Deliverables being developed, by having its Project Manager provide the other party with a written request or recommendation for changes in writing, signed by such requesting party (each a "**Change Request**"). The party receiving the Change Request shall provide a written response to the Change Request, signed by such receiving party, on the same form (a "**Change Response**") in the manner specified below. Each Change Request and associated Change Response (if any) expressly accepted by the non-requesting party as evidenced by its signature on the applicable Change Control Form shall be deemed a "**Change Order**," unless the non-requesting party has proposed changes to the original Change Request from the requesting party that require the non-requesting party's acceptance by execution of the revised Change Request, which, upon execution by the initially requesting party without change, shall be

deemed a "Change Order." Change Requests, Change Responses and all resulting Change Orders shall be in the form attached to this Agreement as Exhibit E (the "**Change Control Form**"). Any Change Request that is not responded to by the receiving party shall be deemed rejected. Any Change Request not responded to by the non-requesting party as provided below shall be deemed rejected.

5.3 Contractor Requested Change. If the Change Request is submitted by Contractor to State, the Change Request shall, to the extent known at the time of the request, indicate schedule changes and any other items Contractor believes the Change Request is likely to impact (each an "**Impact Analysis**"). If a complete and final Impact Analysis cannot be specified, or if aspects of the Impact Analysis cannot be determined at the time of the request, Contractor shall so indicate on the applicable Change Control Form, including a detailed explanation of the basis of such inability of Contractor to so determine. State shall indicate its acceptance or rejection of the Change Request and/or provide a counter-proposal to the Impact Analysis stated thereon via a Change Response. In no event shall any Contractor-submitted Change Request include any additional charges or purport to increase any of the fees set forth on the Fee Schedule payable by a State Entity hereunder. A Contractor submitted Change Request shall not become a Change Order unless such Change Request (and its related Impact Analysis) are expressly accepted by State as evidenced by its signature on the applicable Change Control Form.

5.4 State Requested Change. If the Change Request is submitted by State to Contractor, then Contractor shall provide an initial response to the Change Request within three (3) business days of the receipt of the Change Request or such other time specified by State that is reasonable and appropriate to the scope of such requested change. Contractor shall provide in its initial Change Response a detailed Impact Analysis, or a date by which such detailed Impact Analysis will be provided in a later Change Response. If a complete and final Impact Analysis cannot be specified, or if aspects of the Impact Analysis cannot be determined, at the time of the Change Response, Contractor shall so indicate in its Change Response, including a detailed explanation of the basis of such inability of Contractor to so determine. In no event shall any State-submitted Change Response become a Change Order unless such Change Response (and its related Impact Analysis) are expressly accepted by Contractor as evidenced by its signature on the applicable Change Control Form.

5.5 Limits on Discretion. Notwithstanding any contrary term in this Section, Contractor may not decline to accept any Change Request that: (a) State reasonably believes would reduce the cost of performance, provided that an equitable adjustment in compensation is made for the reasonable out-of-pocket costs of any performance or preparation already undertaken for the original, pre-change Solution, Services, or other Deliverables; or (b) increases Contractor's internal cost or magnitude of required performance, provided that the requested changes are reasonable in scope and the parties agree upon a commensurate increase in compensation to the extent otherwise permitted by this Agreement.

5.6 Status of Change Orders. Each Change Order shall become a part of the Solution Order or Services Order to which it relates as if initially entered into as part of that Services Order, and, together with such Solution Order or Services Order, shall be governed by this Agreement. The parties may mutually agree to supersede, modify, or amend these change control procedures in writing under a Solution Order or Services Order, provided they make express reference to this Section or portion thereof being superseded, modified or amended. If there are conflicts between (or ambiguities within) any Solution Order or Services Order and a subsequent Change Order proposing the delivery of specific Solution, Services, or other Deliverables, the Change Order shall control. If there are conflicts between Change Orders, the most recent Change Order shall control.

6. PERSONNEL.

6.1 Relationship Manager. Contractor shall appoint a qualified member of its staff to act as a dedicated manager of Contractor's relationship with State (the "**Contractor Relationship Manager**"), whose duties shall be to act as primary liaison between Contractor and State for all matters relating to Contractor's performance, and the performance of all Contractor Solution Partners, under this Agreement, who shall have sufficient authority to grant or communicate the granting of all necessary approvals and who shall: (a) have overall managerial responsibility for the responsibilities of Contractor and all Contractor Solution

Partners under this Agreement; (b) have direct access to the key decision makers of Contractor and all Contractor Solution Partners; and (c) be able to call upon the experience, expertise and resources of Contractor and each Contractor Solution Partner as needed to properly, efficiently and timely perform their duties under this Agreement. The Contractor Relationship Manager shall be a resource in addition to any Project Manager or project management established under any Solution Order or Services Order. State may, at its option, designate one or more individuals who shall use reasonable efforts to facilitate Contractor in carrying out an efficient delivery of Services (“**State Relationship Managers**”). Both parties shall notify the other party of a change in the identity of their respective Relationship Managers.

6.2 Contractor Personnel. The individuals who perform Services, whether employees or independent contractors of Contractor (or of a Contractor Solution Partner) are hereinafter referred to as “**Contractor Personnel**” and at all times meet the requirements set forth below. If Services are to be performed outside of the United States all Contractor Personnel shall meet these requirements to the maximum extent applicable, and shall further meet, to the maximum extent applicable, equivalent requirements under local law. The Contractor Personnel assignment requirements are as follows:

(a) Unless specifically agreed otherwise by State in each instance, Contractor shall only assign as Contractor Personnel employees of Contractor and those limited non-employees of Contractor who qualify as “independent contractors” or “temp employees” by meeting the following respective criteria: (i) they are consultants who provide services to Contractor or its entities in the ordinary course of business under independent contractor relationships of a type commonly referred to in the United States as “1099” relationships, or (ii) they are individuals who provide services to Contractor or its entities on a leased employee or so-called staffed- or temp-employee basis pursuant to contracts between Contractor and the third-party staff augmentation companies or staffing companies, and (iii) they are, in all cases, subject, in their individual capacities, to written duties of confidentiality and obligations to protect State’s Intellectual Property Rights that are at least as protective of State as those contained in this Agreement;

(b) Prior to assigning any individual to perform the Services in the United States (which may have been completed at the time of hire), Contractor shall perform a background check, such check shall include the (i) United States Department of Motor Vehicles; (ii) credit check; (iii) national criminal check; (iv) government excluded parties list; (v) the United States Department of Health excluded parties list; (vi) (vi) a determination that the individual’s employment complies with relevant immigration law; and (vii) Contractor shall obtain finger prints for all Contractor Personnel reasonably expected to have access to Confidential Information of any State Entity in connection with such individuals performance of Services hereunder. All information obtained by Contractor pursuant to this Section shall remain in Contractor’s possession and Contractor shall not be obligated to disclose such information to State; and

(c) Contractor shall not assign any person to perform Services who (i) refuses to submit to such checks; (ii) has in the last seven (7) years been convicted of a financial-related crime or a felony (excluding motor vehicle-related offenses); (iii) does not meet the requirements under immigration law to be employed. Contractor shall not be responsible for information not disclosed pursuant to the foregoing background check requirements.

6.3 State Review and Acceptance. If any Contractor Personnel performing Services is found to be unacceptable to State for cause, including demonstration that he or she is not qualified to perform the Services assigned, State shall notify Contractor of such fact and Contractor shall immediately remove said Contractor Personnel and, if requested by State, provide a qualified replacement. If any Contractor Personnel is found to be unacceptable to State for any other reason, State shall notify Contractor of such fact in writing, and Contractor shall promptly take reasonable and appropriate action.

6.4 Project Managers. Contractor shall designate a project manager (“**Project Manager**”) who shall be principally responsible for owning and ensuring timely delivery of the Solution or provision of the Services, as applicable.

6.5 Continuity. If Contractor reassigns any Contractor Personnel, Contractor shall promptly provide a qualified replacement acceptable to State, and State shall not be charged for any training or transition time

for such replacement. Without limiting the generality of the foregoing, because the progress of a project specified in a Solution Order or Services Order may be dependent on such continuity, certain individual Contractor Personnel may be identified in a Solution Order or Services Order as key personnel (“**Key Personnel**”). Except as directed by State under Section 6.3 or for the reasons provided in this Section 6.5, Contractor shall not remove or reassign any Key Personnel at any time for any reason during the term of such individual’s obligations of performance of Services under the applicable Solution Order or Services Order without State’s prior written consent, such consent not to be unreasonably withheld. Contractor shall have the right to re-assign any Key Personnel in case of: (a) death, (b) disability, (c) bona fide termination of employment, (d) changes in Applicable Law, (e) changes in immigration status not caused by the negligence of Contractor or the applicable individual and which could not have otherwise been reasonably foreseen, or (f) upon the occurrence of events having a significant personal impact on the affected Key Personnel (such as death of next of kin). Any re-assignment shall be so permitted only to the limited extent and for such limited duration as required to reasonably accommodate the circumstances of the adversely affected Contractor Personnel.

6.6 Resource Prioritization. If there is any conflict in the resource demands between State and the other State Entities (or among the other State Entities), Contractor shall escalate such conflict to the Contractor Relationship Manager and State Relationship Manager immediately upon becoming aware of its existence, and the respective Relationship Managers shall work with the applicable Project Managers to determine appropriate prioritization and allocation of Contractor Personnel.

6.7 Subcontractors; Ineligible Status. The unique abilities, knowledge, and skills of Contractor and Contractor Personnel constitute a material inducement for State entering into this Agreement. Contractor agrees that it shall not employ any agent or subcontractor in connection with the performance of any Services without the prior written consent of State, which consent may not be unreasonably withheld. If State does consent, Contractor shall provide State with written evidence (acceptable to State) of said agent’s or subcontractor’s compliance with the confidentiality and intellectual property provisions of this Agreement prior to the disclosure of any State Confidential Information to, or the performance by, any such agent or subcontractor in connection with or pursuant to this Agreement. Contractor certifies that the Contractor and/or any of its subcontractors have not been debarred, suspended, or declared ineligible by any agency of the State of Georgia or as defined in the Federal Acquisition Regulation (FAR) 48 C.F.R. Ch.1 Subpart 9.4. Contractor will immediately notify State if Contractor is debarred by State or placed on the Consolidated List of Debarred, Suspended, and Ineligible Contractors by a federal entity. Contractor’s use of any subcontractors does not relieve Contractor of its representations, warranties or obligations under this Agreement. Without limiting the foregoing, Contractor will: (i) be responsible and liable for the acts and omissions of each of its subcontractors (including Contractor Personnel and Contractor Solution Partners) to the same extent as if such acts or omissions were by Contractor or its employees; and (ii) be responsible for all fees and expenses payable to, by or on behalf of each subcontractor in connection with this Agreement, including, if applicable, withholding of income taxes, and the payment and withholding of social security and other payroll taxes, unemployment insurance, workers’ compensation insurance payments and disability benefits.

6.8 Site Visits. Upon the giving of at least five (5) business days’ notice to Contractor, State Entity personnel shall have the right to visit the offices of Contractor and/or the Contractor Solution Partners in order to observe the performance of any Services at the sole cost of the applicable State Entity. The State Entities shall cooperate with Contractor to ensure that such site visits do not unreasonably interfere with Contractor’s normal business operations.

6.9 Timely and Quality Performance. The Contractor Personnel shall perform the Services with promptness and diligence, and in all events by the times specified therefor in the applicable Solution Order or Services Order, if any. At all times during the Term Contractor shall retain sufficient number of Contractor Personnel, with the required skills, to meet the ongoing needs of State and ensure that Contractor achieves the timely implementation of the Solution, including the Guaranteed Functionality and Guaranteed Performance. Contractor shall be responsible for the management of all Contractor Personnel in the performance of Services, the integrity and quality of all Services and Deliverables, and the required periodic reporting of the status of all Services and Deliverables to State. In response to any feedback or

performance assessment provided by State to Contractor Personnel, Contractor shall provide State written acknowledgement within three (3) business days of receipt of the assessment and a comprehensive response including a formal mitigation action plan within ten (10) business days of receipt of the assessment addressing each of the identified areas requiring Contractor improvement.

7. COMPLIANCE.

7.1 State Policies and Directives. Contractor shall ensure that all Contractor Personnel, while at a State Site, will abide by all reasonable policies and directives issued by State, including those relating to its Code of Business Conduct, all on-site rules of behavior, work schedules, security procedures, and other standards and procedures as may be established by State from time to time, provided such policies or directives are published (or otherwise made know) to Contractor prior to such visit and are limited to administrative and security-based issues. Accordingly, Contractor hereby agrees that prior to sending any Contractor Personnel to work at any State facility, Contractor will provide such Contractor Personnel with a copy of all written State policies and procedures provided by State to Contractor and will have Contractor Personnel review and acknowledge same. In addition, Contractor will cause all Contractor Personnel to comply, when at a State Site, with such standard safety policies applicable to such site and such additional policies as State may, from time to time, communicate to Contractor or Contractor Personnel.

7.2 Cyber Security Audits and Reporting.

7.2.1 Contractor has an established information security program containing appropriate administrative, technical and physical measures to prevent data (including Regulated Information (as defined in Section 11.5 below) that Contractor may have access to or be processed by the Solution) against accidental, unauthorized, or unlawful loss, destruction, alteration, disclosure or access consistent with applicable laws. Contractor, on at least an annual basis, shall, at Contractor's expense, participate in a risk assessment relating to Contractor's controls that ensure data security and reduce cybersecurity threats from being realized conducted by an independent third-party agreed upon by State. During the Term Contractor will promptly provide to State a summary of each such assessment that is performed by or on behalf of Contractor, which summary may be redacted to exclude information unrelated to the Solution or Services provided under this Agreement. More specifically, Contractor or its auditor will provide to State at least one (1) hard copy and one (1) electronic copy of the summary from each such assessment at no charge. Contractor, at its own expense, will undertake such actions, and implement such changes, as reasonably necessary to remedy any material deficiencies, concerns or recommendations identified through any audits, examinations, or tests described in this Section 7.2.1 and ensure Contractor's continued compliance with Contractor's obligations as relate data security under this Agreement.

7.2.2 Contractor further agrees that it shall:

(a) Provide the State Entity with the name and contact information for the Contractor's primary information security contact.

(b) Notify the State Entity's primary security contact of an actual or security breach or the suspicion of the occurrence of a security breach (hereinafter a "**Breach Incident**") as soon as practical but no later than forty-eight hours after Contractor becomes aware of a Breach Incident by contacting the primary business and security contact at the State Entity by both telephone and email as agreed upon.

(c) Upon the State Entity's written request and no less than 10 business days following such written request, Contractor shall permit State Entity's information security office to conduct or oversee an audit of the Contractors facilities and/or practices to confirm compliance with this Agreement as well as any applicable laws. Contractor is not required to permit the State Entity to conduct or oversee more than one audit per calendar year unless the process, technology, or services change prior to the next audit or there has been a Breach Incident. All costs associated with such audits shall be the responsibility of the State Entity.

(d) At any time during the term of this Agreement at the State Entity's written request, or upon termination of the expiration of this Agreement for any reason, Contractor shall instruct all authorized persons to promptly and securely return or destroy any and all State Entity data, whether in written, electronic, or other form of media.

7.3 Applicable Law – Contractor. Contractor shall obey and abide by all Applicable Laws, regulations, ordinances and other rules of the United States of America, and any other jurisdiction where Services are, or may likely be, performed in connection with this Agreement (including respective states, territories or subdivisions thereof or any other duly constituted public authority in any such jurisdiction). Without limiting the generality of the foregoing:

7.3.1 Contractor will ensure that no labor will be used in the performance of this Agreement that violates the child labor laws of any country in which State or any State Entity is located or any country in which Contractor is located or performs Services hereunder. If State believes that Contractor is using such labor, then State may immediately terminate this Agreement in which event State shall have no liability whatsoever to pay compensation to Contractor, including for Services already performed.

7.3.2 Contractor represents and warrants that: (i) Contractor, Contractor Affiliates, and any and all of their respective parents, subsidiaries, officers, directors, employees (including all Contractor Personnel), and all of their agents and business partners (collectively, "**Contractor Parties**") are in compliance with, in good standing under, and have not violated, any United States laws or the laws of any other country or countries relating to the transfer of technology, including the Export Administration Regulations, the International Traffic in Arms Regulations and the regulations administered by the Office of Foreign Assets Control of the United States Department of the Treasury or other similar laws or any foreign country (collectively, the "**Transfer Control Laws**"); (ii) Contractor Parties are not, and never have been, named as a "debarred" party, "denied person or entity", "embargoed entity" or otherwise sanctioned under, or prohibited from engaging in activities subject to, the Transfer Control Laws; and (iii) Contractor will immediately notify State in the event that any of the Contractor Parties are named as a "debarred" party, "denied person or entity," or "embargoed entity," or otherwise sanctioned under, or prohibited from engaging in activities subject to, the Transfer Control Laws; and (iv) Contractor Parties will comply with all applicable Transfer Control Laws.

7.3.3 Contractor acknowledges and understands that improper use of material non-public information may be a violation of the law, including the laws concerning insider trading, and may subject it and its employees to prosecution, civil liability, fines and criminal penalties, and, where applicable, may also be grounds for termination of this Agreement.

7.3.4 The Contractor Parties shall comply with all applicable federal, state, and local laws, rules, ordinances, regulations and orders now or hereafter in effect when performing under this Agreement, including without limitation, all laws applicable to the prevention of discrimination in employment and the use of targeted small businesses as subcontractors or contractors.

7.3.5 Certain equipment, software, and technical data which may be provided hereunder may be subject to export and re-export controls under the U.S. Export Administration Regulations and/or similar regulations of the United States or any other country. Contractor shall be responsible for complying with all export and re-export laws and regulations, including: (i) local license or permit requirements, (ii) export, import, and customs laws and regulations, which may apply to certain equipment, software, and technical data provided hereunder; and (iii) all applicable foreign corrupt practices acts.

7.3.6 The Contractor Parties shall comply with all federal, state, and local laws regarding business permits and licenses that may be required to carry out the work performed under this Agreement. The Contractor Parties shall also comply with all policies and standards of the State Entities in effect during the performance of this Agreement, including but not limited to the State Entity's policies and standards relating to personnel conduct, security, safety, confidentiality, and ethics. Further, the provisions of O.C.G.A. Section 45-10-20 et seq. have not and must not be violated under the terms of this Agreement.

7.3.7 Contractor shall obtain and maintain, and shall cause its subcontractors to obtain and maintain, all approvals, permissions, permits, licenses, and other documentation required to comply with all Applicable Laws, rules, or regulations. Contractor certifies that Contractor is not currently engaged in, and agrees for the duration of this Agreement not to engage in, a boycott of Israel, as defined in O.C.G.A. § 50-5-85. Contractor agrees that any failure by Contractor or Contractor's employees to comply with any of the obligations of this section may be treated by the State Entity as a material breach of this Agreement by the Contractor.

7.3.8 Contractor hereby certifies as follows:

(a) Contractor will not engage in the unlawful manufacture, sale, distribution, dispensation, possession, or use of a controlled substance or marijuana during the performance of this Agreement.

(b) If Contractor has more than one employee, including Contractor, Contractor shall provide for such employee(s) a drug-free workplace, in accordance with the Georgia Drug-free Workplace Act as provided in O.C.G.A. Section 50-24-1 et seq. throughout the duration of this Agreement.

(c) Contractor will secure from any subcontractor hired to work on any job assigned under this Agreement the following written certification: "As part of the subcontracting agreement with (Contractor's Name), (Subcontractor's Name) certifies to the contractor that a drug-free workplace will be provided for the subcontractor's employees during the performance of this Agreement pursuant to paragraph 7 of subsection (b) of Code Section 50-24-3."

7.3.9 Contractor may be suspended, terminated, or debarred if it is determined that any of Contractor's certifications in Section 7.3.8 is false or Contractor has violated any such certification by failure to carry out the requirements of O.C.G.A. Section 50-24-3(b).

7.4 Permits and Licenses. Contractor acknowledges and agrees that it is solely responsible for procuring and maintaining all necessary permits and licenses required in connection with Contractor's performance, and the performance of all Contractor Solution Partners, under this Agreement, including obtaining all necessary shipping and/or delivery permits and processing and procuring all necessary visas and passport documents for all Contractor Personnel in advance of their assignment in connection with Services. Contractor will obtain, at Contractor's sole cost and expense, all such permits, licenses and visas in a timely manner to avoid any unnecessary delay.

8. PERFORMANCE STANDARDS, MONITORING AND MEASUREMENT.

8.1 Performance Levels. Contractor shall provide the Solution and perform the Services with promptness and diligence, and in all events by the times specified therefor in the applicable project documentation, Solutions Order, or Services Order as applicable. Contractor shall be responsible for the management of all Contractor Personnel in the performance of Services, the integrity and quality of all Services and all applications and Deliverables, and the required periodic reporting of the status of all Services and such applications and Deliverables to State. In fulfilling its obligations under this Agreement, Contractor shall perform, and shall cause each Contractor Solution Partner to perform, all Services and all Deliverables to perform, in accordance with the response, resolution, and other support standards and timelines and such other systems availability and processing requirements as are set forth in the applicable Services Order (the "**Performance Levels**"). If State management, including the State Relationship Manager or Project Manager, provides feedback or performance assessments that identify areas requiring Contractor improvements, Contractor shall provide State written acknowledgement within three (3) business days of receipt of the assessment and a comprehensive response, including a formal mitigation action plan, within ten (10) business days of receipt of the assessment addressing each of the identified areas requiring Contractor improvement.

8.2 Non-Conformance.

8.2.1 Generally. If Contractor or any Contractor Solution Partner fails to meet any Performance Level or fails to perform its other obligations hereunder, Contractor shall immediately: (a) investigate and report to State on the causes of the failure; (b) prepare an action plan for State's approval to correct the failure; (c) advise State, as and to the extent requested by State, of the status of remedial efforts being undertaken with respect to such failure; (d) correct the failure and begin meeting the Performance Levels; and (e) take appropriate preventive measures so that the failure does not recur. In addition, failures to meet a Performance Level shall entitle State to receive liquidated damages and/or credits (as applicable) from Contractor, as provided in the applicable Services Order.

8.2.2 Reserved.

8.3 Measurement Tools. Contractor shall utilize, and shall cause the Contractor Solution Partners to utilize, the necessary measurement and monitoring tools and procedures required to measure and report its performance against all Performance Levels. Such measurement and monitoring shall permit reporting at a level of detail sufficient to verify compliance with the Performance Levels. Contractor shall provide State with information and access to such tools and procedures, upon request, for purposes of verification. State also shall monitor and measure certain Performance Levels, and any discrepancy between Contractor and State measurements of the Performance Levels shall be resolved by reference to State's measurement and monitoring tools and procedures.

8.4 Proactive Monitoring. Contractor acknowledges and agrees that the performance of Services in accordance with this Agreement is critical to State's business and that State requires metrics to monitor such performance. Accordingly, at no cost to State, Contractor shall, and, if requested by State shall cause each Contractor Solution Partner to: (a) provide to State, on a quarterly basis, data (or metrics) regarding its progress in improving the quality and productivity of Contractor Personnel providing services pursuant to or in connection with this Agreement, including data on the number of Contractor Personnel, average experience, and turnover (on a project basis); (b) provide to State, on a quarterly basis, data on each project covering such matters as productivity, quality and timeliness, new development productivity measures (function points per person/day, error rates per function point, etc.) and maintenance project measures (requests serviced weekly etc.); and (c) provide to State a log reflecting State open issues that is to be updated on a monthly basis. In addition to the periodic delivery described above, Contractor agrees to provide State with the foregoing information within fifteen (15) days of a request made by State for the same.

8.5 Coding Standards. If Contractor or a Contractor Solution Partner will be performing development, programming or other coding services under a Services Order and the Deliverables thereunder will be owned exclusively by State (pursuant to Section 12 below), Contractor or the applicable Contractor Solution Partner shall, with respect to such Services Order, be responsible for such specific coding and naming standards and conventions as may be provided by State in connection with certain of its and/or its third-party licensors' requirements, as well as such quality performance and productivity provisions and documentation requirements, if any, set forth in the applicable Services Order. Contractor shall, in addition, be responsible for imposing the applicable quality assurance requirements on Contractor Personnel. State shall have the right to conduct quality audits and to perform or witness inspections or tests of the Deliverables furnished hereunder at Contractor's facility, at sole cost of State, at any time during development and prior to delivery. Notwithstanding anything contained in this Agreement to the contrary, State for itself, and on behalf of the other State Entities, acknowledges and agrees that the Solution shall not constitute "works made for hire", and shall remain the exclusive property of Contractor.

8.6 Quality Assurance. State may, at its option, employ consultants, including quality assurance consultants, for periodic review of any work or project, including evaluation of Change Orders and monitoring of compliance with Service Level Agreements and Performance Levels. References to State in this Agreement shall include such consultant to the extent State so indicates for that purpose. If so requested by State, State shall have the right to receive and review quality assurance reports produced by Contractor. Contractor shall accommodate reasonable State requests to expand or modify Contractor's quality assurance procedures for Projects in progress.

8.7 **Material Defects.** Contractor shall give State prompt notice if Contractor becomes aware of a material defect in any Deliverables or the performance of any Services or any issue that may affect Contractor's ability to implement the Solution, including all Guaranteed Functionality and Guaranteed Performance, in accordance with the timeline required by this Agreement.

9. **DELIVERY AND ACCEPTANCE.**

Each delivery and implementation of the Solution and Services or any additional applications at a State Site shall be subject to acceptance by State in accordance with acceptance testing procedures, as provided in the Solutions Order. An "**Acceptance Testing Plan**" for the Solution and Services shall be prepared by Contractor and submitted to State prior to execution of this Agreement, which agreement, as approved by State shall be incorporated into this Agreement. The Acceptance Testing Plan shall be based on full implementation of the Solution and Services and shall include testing procedures sufficient to demonstrate that (a) all functionality has been provided and performs in the applicable State Entity's environment, in all material respects, in accordance with the Guaranteed Functionality; (b) the applications and deliverables meet the warranty requirements specified in this Agreement and the applicable Solution Order; (c) the applications and Deliverables will perform at acceptable levels required to support State's implementation of the SVS and the operation of general and primary elections using such SVS; and (d) the applications and Deliverables will successfully complete an "election voting and processing" simulation. Testing procedures will include testing before, at, and after "go-live" as appropriate before the Solution "goes-live", but the testing will continue after "go-live" as appropriate to verify that the applications and services meet applicable requirements in a full production mode. State representatives will have the right to be present during the Acceptance Test and review all test results. When the applications and Deliverables meet the requirements of the Acceptance Test, State will provide a written sign-off that Acceptance has occurred. If the applications and Deliverables fail to meet all material requirements of the Acceptance Test, Contractor will, at its sole expense, correct the deficiencies and the Acceptance Test will then be repeated. Acceptance will not relieve Contractor of responsibility for its warranties, support and maintenance obligations, or achieving the Performance Levels.

10. **CHARGES, PAYMENT, AND TAXES.**

10.1 **Payments.** As further provided in Contractor's fee proposal delivered by Contractor, accepted by State prior to execution of this Agreement, and attached hereto as Exhibit G (the "**Fee Schedule**"), and subject to the other terms and conditions of this Agreement, in consideration of Contractor's agreement to provide the Solution to State, deliver necessary documentation, train State Personnel, and render related services in accordance with this Agreement, Contractor shall be entitled to be paid as follows (each a "**Milestone Payment**" unless otherwise noted):

- 10.1.1 \$44,967,752.40 on the Effective Date, inclusive of initial implementation/training and initial Equipment costs.
- 10.1.2 \$1,500,000.00 for training and implementation upon Certification of the November 2019 Election.
- 10.1.3 \$4,386,020.40 for remaining costs for training and implementation upon Certification of the March 2020 Presidential Preference Primary Election.
- 10.1.4 \$1,500,000.00 for final training and implementation and hold back upon Certification of the November 2020 Election.
- 10.1.5 \$834,673.35 upon Final Acceptance of election management system hardware and software to the State.
- 10.1.6 \$816,768.00 upon Final Acceptance of ImageCast Precinct scanners (without ballot box) and ImageCast Central scanners hardware and software for absentee/mail ballot voting.

10.1.7 The following items will be invoiced on a monthly basis upon unit Final Acceptance by the State:

- (a) Electronic Pollbook hardware and software at a \$708.93/unit for a total cost of \$5,671,440.00.
- (b) ImageCast Precinct scanners hardware and software at \$2,330.36/unit for a total cost of \$8,156,260.00.
- (c) ImageCast X BMD hardware and software at the remaining unit cost* of \$753.53 for a total cost of \$22,102,676.50.

* Remaining Cost reflects an overall reduction resulting from the initial milestone payment equaling \$44,967,752.40 for initial implementation and ImageCast X BMD costs.

10.1.8 Equipment Charges. The price for the Equipment ordered by a State Entity, as contemplated by the Fee Schedule, shall be set out in each applicable Solution Order (the "**Equipment Charges**"). Contractor shall deliver an invoice for the relevant Equipment Charges to the applicable State Entity in accordance with the following: (a) fifty percent (50%) of the Equipment Charges following State's completion of initial Acceptance Testing and (b) the remaining fifty percent (50%) of the Equipment charged upon the applicable State Entity's confirmation that testing of the same has been satisfactorily completed at the State Site at which such Solution is to be implemented and administered as designated by the applicable State Entity. Notwithstanding anything contained herein to the contrary the parties acknowledge and agree (i) that purchases of new models of Equipment released by Contractor shall be made available to the State Entities at the same price as the Equipment purchased as part of the Solution Order dated as of even date herewith, provided, if the State Entities shall not be obligated to upgrade to such new models and if any State Entities do not elect to purchase such new models, Contractor shall continue to support the version of the Equipment then in use by the State Entities, including ensuring that such Equipment is supported by the Software.

10.1.9 T&M Rates. Except as otherwise set forth in the Fee Schedule, this Agreement does not contemplate, and Contractor shall not be entitled to, payment for any of its work, overhead, or expenses on a time and materials basis.

10.2 Events Affecting Critical Milestones - Liquidated Damages. By entering into this Agreement, Contractor acknowledges and agrees that in the event that State determines in good faith that Contractor has not meet a Critical Milestone by the applicable Milestone Deadline, the State will suffer actual damages that will be impractical or extremely difficult to determine and the State shall be entitled to recover agreed upon liquidated damages in an amount equal to \$1,000 for each calendar day after the applicable Milestone Deadline until the Critical Milestone in question has been satisfactorily completed by Contractor. Contractor further acknowledges and agrees that the amounts to which State may become entitled under this Section 10.1 are not penalties but a fair and reasonable estimate of the anticipated harm that may be caused to the State Entities by delays that result in Contractor failing to meet the Milestone Deadlines for Critical Milestones provided that such liquidated damages be deemed to be constitute State's sole remedy, exclusive or otherwise, for any damages caused by such a failure and shall be in addition to any other monetary and non-monetary remedies available to State under this Agreement, at law or in equity. Notwithstanding anything contained in this Agreement to the contrary, in the event that the State becomes entitled to any amount under this Section 10.1, State may, in its sole discretion, set off the sum owed it against any sum owed to Contractor under this Agreement or any other contract between the State and Contractor.

10.3 Invoices. Contractor shall submit invoices to the applicable State Entity (a) thirty (30) days prior to the anticipated completion of the applicable Installation Event to which a Milestone Payment relates; and (b) with respect to Equipment Charges, in accordance with Section 10.1.8. The applicable State Entity shall pay all undisputed correct invoices, which are timely submitted to it, within thirty (30) days of receipt.

10.4 Disputed Charges. In the event State reasonably believes that any invoice submitted by Contractor contains any discrepancies or errors, State shall notify Contractor of such discrepancy(ies) or error(s). The parties agree to cooperate in good faith to resolve any dispute in a timely manner. Upon receipt of State's notification of dispute, Contractor will investigate such dispute and will either (a) correct such invoice if a correction is so required and provide a corrected invoice or other such notice in writing, or (b) if no correction is required, send State written notice that Contractor has investigated such dispute and that Contractor considers the amounts due and payable and no longer in dispute. State shall not be required to make payment on any disputed portion of an invoice until such time as the dispute has been finally resolved by the parties. For the avoidance of doubt, a dispute regarding an invoice and State withholding payment of disputed charges as permitted under this Agreement will not permit Contractor to suspend or cease performance of the Services and Contractor shall continue to provide such Services.

10.5 Currency; Settlement Method. State shall settle payments with Contractor by wire transfer or such other payment method as mutually agreed by the parties.

10.6 State Status as Most Favored Customer. During the Term, Contractor shall offer to State and the other State Entities the Solution and any other Services which Contractor offers on a general basis to its other customers, at prices at least as favorable as Contractor offers or provides to any Person that orders similar products and quantities as ordered by State pursuant to Solution Order No. 1. In comparing the prices offered by Contractor to other customers with the prices offered to State under this Agreement the fees paid by State hereunder for the applicable Solution shall be reduced by an appropriate amount to compensate for any installation, training, migration and other services provided by Contractor hereunder at no charge and to account for any credits provided by Contractor to State hereunder. The Contractor shall give prompt written notice to the State of each such instance in which more favorable fees as described above are extended to another State. On each anniversary of the Effective Date and at such other time as the State may request (based on the State's reasonable belief that the Contractor has an obligation under this Section), the Contractor shall deliver to the State a certificate duly executed by an appropriate executive of the Contractor, certifying that, as of the date of such certificate, and at all times since the date of the last certification pursuant to this Section (or since the Effective Date if there has been no prior certification), stating that the Contractor is and has been in compliance with this Section. If the Parties are unable to agree as to the Contractor's compliance with the requirements of this Section or, as to the appropriate means to effectuate this Section, then such issue shall be determined pursuant to Section 17.5.

10.7 No Other Charges; Expenses. Contractor acknowledges and agrees that the charges and fees described in this Section 10 shall be "all-inclusive" and represent the total cost for the Solution including all costs associated with all goods, software, and services to be provided Contractor pursuant to this Agreement, including (i) the SVS components described on each Solution Order, (ii) all Equipment described in the applicable Solution Order, (iii) the Training Services described in such Solution Order, and (iv) the Extended Warranty and all maintenance, support, and remedial action thereunder required to ensure the Solution and all components thereof are available to the ordering State Entity and function in accordance with the requirements of this Agreement. In no event shall State be liable for any amounts not described in this Section 10 or any other charges, fees, expenses, or costs incurred by Contractor, which Contractor failed to consider in its eRFP Response. Accordingly, no such expenses of any Contractor Party will be separately reimbursable by any State Entity.

10.8 Taxes.

10.8.1 State is exempt from Federal Excise Taxes, and no payment will be made for any taxes levied on Contractor's employee's wages. State is exempt from state and local sales and use taxes on the Services. Tax exemption certificates will be furnished upon request. Contractor or an authorized subcontractor has provided State with a sworn verification regarding the filing of unemployment taxes or persons assigned by Contractor to perform Services required in this Agreement, which verification is incorporated herein by reference.

10.8.2 By executing this Agreement the Contractor certifies it is either (a) registered with State Department of Revenue and collects and remits State sales and use taxes as required by Georgia law,

including Chapter 8 of Title 48 of the O.C.G.A. or (b) not a “retailer” as defined in O.C.G.A. Section 48-8-2. The Contractor also acknowledges that State may declare this Agreement void if the above certification is false. The Contractor also understands that fraudulent certification may result in State or its representative filing for damages for breach of contract.

10.9 Books and Records.

10.9.1 GAAP Standards; Record Retention. Contractor shall maintain books and records in accordance with Generally Accepted Accounting Principles to substantiate Contractor’s prices and other charges billed to State under this Agreement and each Solution Order and Services Order. Contractor will maintain such books and records for a period of at least five (5) years following the date of final payment or completion of any required audit, whichever is later. Records to be maintained include both financial records and service records.

10.9.2 Information Regarding Billing Questions. Contractor shall answer billing questions and provide State with such documentation as State may request pertaining to billing. Once per year and at the sole cost of State, Contractor shall provide State and State’s representatives with reasonable accept access to such books and records for purposes of auditing the fees under this Agreement and/or any Schedule or Services Order.

10.10 Audit. The Contractor shall permit the Auditor of State of Georgia or any authorized representative of State, and where federal funds are involved, the Comptroller General of the United States, or any other authorized representative of the United States government, to audit Contractor to achieve one or more of the following additional objectives: (a) verify the security and integrity of State’s and each other State Entity’s data and examine the systems that process, store, support, and transmit that data or (b) examine Contractor’s performance of, and conformance to the terms of, this Agreement, including, to the extent applicable to the applications and services provided by Contractor and to the charges therefor, performing audits of (i) Contractor’s practices and procedures, including its conformance with State policies with which it is obligated to comply under this Agreement and otherwise as reasonably necessary to enable State to confirm that Contractor is meeting applicable regulatory and other legal requirements for which it is obligated to comply under this Agreement; (ii) supporting information and calculations regarding compliance with Performance Levels, security standards for which Contractor is responsible hereunder or other required standards or levels of performance; and (iii) Contractor’s disaster recovery and back-up procedures. State agrees to the following conditions in connection with such audits: (i) State will not unreasonably interfere with Contractor’s normal business operations, (ii) Contractor is not entitled to review or see and other Confidential Information of other Contractor States except in an anonymized or redacted format, (iii) all information disclosed during such site visit shall be considered Contractor’s Confidential Information (unless the information Contractor possesses is already Confidential Information of State or State Data), and (iv) State will comply with Contractor’s reasonable security policies and procedures delivered in writing to State in advance of the applicable audit. If as a result of any such audit State determines that Contractor has overcharged State, State will notify Contractor of the amount of such overcharge and provide Contractor with a report setting forth the determination of such overcharge. Upon such notice, Contractor shall promptly pay to State the amount of such overcharge, together with interest thereon at the Interest Rate calculated from the date of such overcharge until the date Contractor reimburses State. In addition, if such audit reveals an overcharge to State in any fee, cost, or charge billed by Contractor, Contractor shall reimburse State for the actual costs of such audit. In the case of a performance-related audit, Contractor and State shall meet to review each audit report promptly after the issuance thereof and to mutually agree upon the appropriate manner, if any, in which to respond to the changes suggested by the audit report. State and Contractor agree to develop operating procedures for the sharing of audit and regulatory findings and reports related to Contractor’s operating practices and procedures produced by auditors or regulators of either party. Evidence of criminal conduct uncovered by State during an audit will be turned over to the proper authorities.

10.11 Delay of Payment Due to Contractor’s Failure. If the State Entity in good faith determines that the Contractor has failed to perform or deliver any component of the Solution for which the State Entity is charged as required by the Agreement, the Contractor shall not be entitled to the compensation under this

Agreement corresponding to such components until such components are delivered and/or conform to the requirements of this Agreement. To the extent that the Contractor's failure to perform or deliver in a timely manner causes the State Entity to incur costs, the State Entity may deduct the amount of such incurred costs from any amounts payable to Contractor. State's right to deduct such incurred costs shall not in any way affect State's right to terminate this Agreement or any Solution Order or Services Order.

10.12 Set-Off Against Sums Owed by the Contractor. In the event that the Contractor owes the State Entity and/or the State any sum under the terms of this Agreement, pursuant to any judgment, or pursuant to any law, the State Entity and/or the State may set off the sum owed to the State Entity and/or the State against any sum owed by the State Entity and/or the State to the Contractor in the State Entity's sole discretion.

11. CONFIDENTIALITY, PRIVACY, AND DATA SECURITY.

11.1 Disclosure of Confidential Information. Contractor and State acknowledge that, in the course of performance under this Agreement, one party (the "**Disclosing Party**") may intentionally or inadvertently disclose, deliver, or permit access by the other party (the "**Receiving Party**") to information, data, or materials which are, to the Disclosing Party, secret, proprietary, and/or confidential, including as may be so designated by statute, regulation, or common law, including, among others, by the form of the Uniform Trade Secrets Act adopted under Applicable Law (if any) and various applicable privacy laws. All of the foregoing information, data, and materials are referred to collectively in this Agreement as the "**Confidential Information**" as that term is further defined and described in Section 11.2.

11.2 Confidential Information. Without in any way limiting the generality of the definition of Confidential Information contained in Section 11.1, the term Confidential Information shall also expressly include all data, information, materials, and subject matter, works of authorship, methods, processes, techniques, systems, and know-how containing, recording, expressing, or embodying the Disclosing Party's (a) products, both existing and under development during the Term, and all related documentation algorithms, source code, object code, workflows, models, formulae, structures, schematics, designs, drawings, specifications, and flow charts containing, comprised by or embodied in such products and (b) current or prospective businesses, business plans, states, finances, contracts, contractual arrangements, employees, contractors, partners, investors and suppliers. All of the foregoing shall be Confidential Information hereunder irrespective of its field of use and whether it is (i) owned by the Disclosing Party, leased or licensed from third parties or held for the benefit of or in connection with its clients, states, business partners, or investors; (ii) intangible or tangible, but if tangible, regardless of form, medium or physical format including paper documents or graphic or machine readable media; and (iii) actually disclosed to a party, but if actually disclosed, whether in whole or in part or orally or in writing. Notwithstanding anything contained in this Agreement to the contrary, the parties acknowledges and agree that where Contractor is the Disclosing Party, "Confidential Information" shall include only such information that Contractor has marked as "confidential", "proprietary", "trade secret", or otherwise redacted in accordance with eRFP Section 2.1.12.2.1 et seq. the terms of which are incorporated herein by reference, provided, however State reserves the right to determine if such information has been properly designated as such and whether it may or may not be disclosed by State.

11.3 Non-Disclosure and Non-Use. Except as otherwise permitted by eRFP, the Receiving Party shall hold all Confidential Information actually received in strictest confidence and shall not disclose or provide the Confidential Information to any individual or entity without the express written consent of the Disclosing Party in each instance, except to the Authorized Recipients. In all events the Receiving Party shall handle, store, and maintain all Confidential Information actually received with a degree of care that is reasonable for the circumstances of disclosure and the nature of each component of Confidential Information. The Receiving Party shall not make any use of the Confidential Information whatsoever except such limited uses as are required under the Agreement. To the limited extent reasonably necessary for such permitted purposes, the foregoing right of use shall include the right to make a reasonable number of copies of the Confidential Information each of which shall be subject to Section 11.8. The use rights hereunder do not permit, and the Receiving Party is expressly prohibited from (a) performing any benchmarking or other comparative or competitive analysis of any Confidential Information for any purpose other than as required

under this Agreement and (b) using, distributing, delivering, or disclosing the Confidential Information or any portion to any Person in violation of U.S. export regulations.

11.4 Confidentiality Exclusions. The Receiving Party shall have no obligation under Section 11.3 with respect to any Confidential Information which the Receiving Party can demonstrate by reasonable written evidence contemporaneous with the event of the exclusion sought to be used hereunder: (a) was already known to it at the time of its receipt hereunder; (b) is or becomes generally available to the public other than by means of breach of this Agreement; (c) is independently obtained from a third party (other than any Authorized Recipient) whose disclosure to the Receiving Party does not violate a duty of confidentiality; or (d) is independently developed by or on behalf of the Receiving Party without use of, reference to, or reliance on any Confidential Information. Furthermore State, as Receiving Party shall have no obligation under Section 11.3 with respect to any information that State determines is required to be disclosed by Applicable Law including the provisions of the Georgia Procurement Manual, State Purchasing Act, or Georgia Open Records Act as provided in O.C.G.A. Section 50-18-70 et seq. If the Receiving Party is required by a court or other body of competent jurisdiction to disclose the Confidential Information, the Receiving Party may disclose only so much Confidential Information as is legally required, provided that the Receiving Party has given notice of such compelled disclosure to the Disclosing Party and has given the Disclosing Party a reasonable opportunity to object to such disclosure and has provided reasonable assistance, at the cost of the Disclosing Party, in obtaining and enforcing a protective order or other appropriate means of safeguarding any Confidential Information so required to be disclosed.

11.5 Privacy Regulations and Guidelines. This Agreement, the Solutions Orders, Services Orders, and the parties hereunder, may be governed by one or more privacy laws, regulations or guidelines including O.C.G.A. 21-2-379.24(g) and such others as may be designated by State from time to time (collectively, the "**Privacy Regulations**"). If so governed, then to the extent not captured already by the definition of Confidential Information hereunder, or required already by the Receiving Party's obligations under Section 11.3: (a) the term "Confidential Information" shall further include all Nonpublic Personal Information, Personal Information, material nonpublic information and Personal Data as each of those terms is defined in or by application of each respective Privacy Regulation (collectively, the "**Regulated Information**"); and (b) the Receiving Party shall comply with all requirements of the Privacy Regulations reasonably known to be applicable to the Regulated Information portions of the Confidential Information actually received by the Receiving Party including all reporting, audit, access, third-party disclosure and onward transfer obligations and restrictions therefor, if any are so applicable. If a Privacy Regulation applicable to the Receiving Party under this Agreement is amended, and/or if any other state or federal law, regulation or treaty is effected such that a more restrictive standard of confidentiality or obligation of privacy or security is imposed with respect to an applicable component of the Regulated Information portions of the Confidential Information, then such more restrictive standard shall prevail over the provisions of this Agreement with respect to those portions. By signing below the Receiving Party acknowledges that the Privacy Regulations may prohibit or render ineffective some or all of the exclusions otherwise available under Section 11.3. Notwithstanding anything to the contrary contained in this Agreement, Contractor agrees (i) it shall maintain, and shall require all Authorized Recipients to maintain, effective information security measures to protect Regulated Information from unauthorized disclosure or use, and (ii) it shall provide with information regarding such security measures upon the reasonable request of State and promptly provide State with information regarding any failure of such security measures or any security breach related to Regulated Information.

11.6 No Transfer of Rights. Nothing in this Agreement is, nor shall be deemed to be, any transfer, conveyance, assignment or waiver (by express license, implied license or otherwise) by the Disclosing Party of any Intellectual Property Rights it has or claims to have in the Confidential Information.

11.7 Data and Network Security.

11.7.1 Contractor is responsible for providing network security and security for such of its facilities where its servers or other network equipment are located. Contractor shall also comply with its own then-current security policies and procedures, and its security policies and procedures shall comply with laws and regulations applicable to Contractor.

11.7.2 If, during the course of this Agreement, Contractor is creating, hosting, maintaining, processing or transmitting any State Confidential Information on or through any Contractor computer networks, data centers, labs, supporting environments, Web servers or other information technology resources (collectively "**Contractor Computer Systems**"), or is otherwise using any Contractor Computer Systems in connection with this Agreement, then with respect to all such Contractor Computer Systems, Contractor will, in accordance with industry best practices or higher standards that are in all cases no less than reasonable:

(a) Limit physical and electronic access to Contractor's employees and essential third-party contractors, on a need-to-access basis, who have signed a written agreement that is at least as protective of the confidentiality and security of State Confidential Information as those provided in this Agreement;

(b) Implement and maintain technical access controls that, at a minimum, require unique identification and authentication of all users, restrict access to all data, software, or other file-system objects exclusively to those users who need such access to perform their job responsibilities, and limit administrator-level control to only authorized IT personnel;

(c) Implement and maintain transmission controls that, at a minimum, allow only the data protocols required for the function and management of each solution to be used or transmitted and insure the confidentiality, availability, and integrity of all transmissions;

(d) Implement and maintain firewall technology and intrusion detection software configured to minimize or eliminate hacking and other threats;

(e) Implement and maintain protection against viruses, worms, Trojan horses, spyware, and other malicious code;

(f) Perform routine reviews of logs files and system records for suspicious activity;

(g) Perform regular reviews of relevant security notifications and alerts (e.g., notifications of bugs, attacks, and patches), and apply such patches and fixes as appropriate;

(h) Implement and maintain disaster recovery, backup, and other contingency plans; and

(i) Conduct regular security audits, reviews, and tests and systematically retain log files, system records, test plans, and other security documentation.

11.7.3 Contractor shall notify State immediately upon discovery or notification of any actual, potential or threatened Security Breach. Contractor agrees to take action immediately, at its own expense, to identify and eradicate (or to equip State to identify and eradicate) any further Security Breach and carry out any recovery necessary to remedy any impact of such Security Breach. Contractor's actions will include at a minimum:

(a) Confirming the attack;

(b) Denying access from the source of the attack;

(c) Investigating and evaluating the extent of the damage, if any;

(d) Backing-up the affected systems and those suspected to be affected;

(e) Strengthening defenses everywhere, not just the suspected path that the attacker used, if possible;

(f) Contacting Contractor's internet service provider and, subject to State's prior written approval, any law enforcement agency to work with Contractor's security team; and

(g) Producing an incident report within twenty-four (24) hours detailing Contractor's findings and distributing the report to State.

11.8 Disaster Recovery – Requirements and Audit Procedure. Contractor shall provide a disaster recovery plan and data backup procedures (the "**Disaster Recovery Plan**") attached hereto as Exhibit J.

11.9 Loss of Information; Equitable Relief. The remedy at law for any breach or threatened breach of this Section 11 shall be inadequate, and in addition to any other remedy available at law, in equity, or under this Agreement, the non-breaching party shall be entitled to seek to obtain injunctive relief without proof of irreparable injury and without posting bond. If there is any unauthorized disclosure or loss of, or inability to account for, any Confidential Information of the Disclosing Party, the Receiving Party shall promptly: (a) notify the Disclosing Party upon becoming aware thereof; (b) take such actions as may be necessary or reasonably requested by the Disclosing Party to minimize the disclosure, losses or violation; and (c) cooperate in all reasonable respects with the Disclosing Party to minimize the violation and any damage resulting therefrom.

11.10 Compliance by Contractor Solution Partners. Without limiting Contractor's obligations above, Contractor shall cause each Contractor Solution Partner to comply with the provisions of this Section 11 to the same extent that Contractor is required to comply with such provisions.

12. OWNERSHIP OF CONTRACTOR PRODUCTS; STATE DATA; THIRD-PARTY PRODUCTS.

12.1 Ownership of Contractor Products. State acknowledges that the Software, the Contractor data bases which are part of the Services, and all copyrights, patents, trade secrets, and other intellectual and proprietary rights therein and thereto (collectively the "**Contractor Products**") are and shall remain the exclusive and confidential property of Contractor or the third parties for whom Contractor is acting as agent or from whom Contractor has obtained the right to use the Contractor Products. For this purpose, the Contractor Products do not include the State Data, including any extract, database, output, reports or derivative works that include or are based on the State Data, or any business or transaction information produced by or for State using the Services or Software (the "**Output**").

12.2 State's Rights in Output. State may use the Output in conjunction with any services, software or equipment that State or State may choose. State or any contractor chosen by State may copy, use, and modify such data as Contractor provides State and the Output for purposes of meeting its internal business requirements. State may make an appropriate number of copies of the Contractor Products provided to State at its premises for back-up purposes only.

12.3 Confidentiality of State Data; File Security. Contractor acknowledges and agrees that any file or other information provided by any State Entity to Contractor, including any extract, database, output, reports or derivative works that include or are based on the State data, or any business or transaction information produced by or for a State Entity using the Services or Software (collectively the "**State Data**") shall be and remain the exclusive and confidential property of State. Except to the limited extent set forth in Section 12.4 below, Contractor shall treat as confidential and will not disclose or otherwise make available any State Data to any person other than employees of Contractor with a need-to-know. Contractor will instruct its employees who have access to the State Data to keep the same confidential by using the same care and discretion that Contractor uses with respect to its own confidential property and trade secrets. Contractor will provide reasonable security provisions to ensure that access to the State Data is available only to State. Contractor will hold and process the State Data of State and State's other vendors in systems that are physically and logically separated from other data of other States.

12.4 Contractor Use of State Data. Notwithstanding the foregoing, but subject to State's consent on a case-by-case basis, State will consider Contractor's request that Contractor be given the right to use such

State Data as it ordinarily receives, and to distribute such State Data to third parties, in an anonymized and cleansed statistical and/or compilation forms in connection with other Contractor services. If so approved by State in writing on a case-by-case basis, State acknowledges that such statistics and/or compilations (which are not identifiable to State or State's location and do not include information otherwise subject to privacy or confidentiality requirements) may be used or resold by Contractor outside the scope of this Agreement.

12.5 Turnover of State Data. If so requested by State at any time before or after termination of this Agreement, Contractor shall provide copies of the State Data in Contractor's possession to State in such form as State may reasonably request together with such tables and instructions as State may require to extract or convert the information. Unless otherwise approved by State or necessary to carry out the transition/termination provisions of this Agreement, Contractor may not retain copies of the State Data following termination of this Agreement.

12.6 Unlimited Use of State Data and Output by State. State and its designees are free to extract, aggregate, use, store, modify, compile, retransmit, and distribute the State Data, including all Output, in any manner and for any purpose that State may desire, without being subject to any restriction on doing so that may be associated with the Contractor applications or any other Contractor Products. State may install and use its own or third-party providers' equipment and software to do so, and State and State may create and install its own or third-party providers' APIs to access and collect any of the State Data or applicable files at State's premises in such manner as State or State chooses.

12.7 Deliverables. The deliverables that Contractor actually provides to the State Entities under this Agreement may take the form of any Solution, the Services themselves or individual items of State-Specific Enhancements, Third Party Materials or Derivative Works & Improvements, or one or more of them. More likely, however, such deliverables, shall be composed of some combination of such Solution, State-Specific Enhancements, Contractor Products, Third Party Materials or Derivative Works & Improvements, or one or more of them created by linking, embedding, bundling or incorporating them with or into one-another. Such combination shall be referred to as "**Deliverables**." Each party shall retain at all times its respective ownership rights of the Intellectual Property Rights in and to such party's respective Proprietary Materials components of the Deliverables under the terms of this Section 12 and neither party shall own the Intellectual Property Rights in and to the Deliverables as a whole. Notwithstanding anything contained in this Agreement to the contrary, State for itself, and on behalf of the other State Entities, acknowledges and agrees that the Solution shall not constitute "works made for hire", and shall remain the exclusive property of Contractor.

12.8 Third Party Materials. Neither Contractor nor any Contractor Personnel shall use any Third Party Materials in the performance of the Services nor introduce, embed, bundle, link, or incorporate Third Party Materials into or with any State Data or Output unless: (a) expressly requested by State or (b) disclosed to State by Contractor in writing in the applicable Solution Order or Services Order in connection with which Contractor desires to use them. If use of Third Party Materials is so permitted, Contractor shall supply them by either providing State: (i) with the applicable shrink-wrap license agreement governing the use of such Third Party Materials or (ii) with the applicable license agreement submitted by the owner or provider of such Third Party Materials generally to its states; or (iii) with all necessary use and/or license rights via pass-through or assignment to State, as well as all warranties and maintenance and support rights (if any) as provided by either the manufacturer of the applicable provider of such Third Party Materials or by Contractor on such manufacturers' behalf pursuant to a reseller or similar agreement therefor.

12.9 Open Source Software. The Solution may contain Third Party Materials subject to or governed by an open source license. Use by State, as part of the Solution, in accordance with this Agreement and normal operating instructions, of such open source license (in object code) procured by Contractor under a license commonly referred to as "open source," "free software," "copyleft," or "community source code license," including, without limitation, the GNU General Public License or Lesser General Public License (collectively, "**OSS**") is and will be in compliance with the terms of such OSS licenses. The use by State of the System in accordance with this Agreement does not require that the OSS included by Contractor in the System will be combined or merged with any proprietary software provided or separately operated by State.

12.10 Residuals. Subject to Section 11 (Confidentiality, Privacy and Data Security), Contractor, State or the applicable State Entities shall have the right to use for any purpose Residuals arising from this Agreement. For the avoidance of doubt, the foregoing shall not be deemed to grant to the receiving party a license to use the other party's copyright, patents, trademarks, source code, or other Intellectual Property.

13. BONDS & INSURANCE.

13.1 Bonds. Within ten (10) days of the Effective Date, Contractor shall obtain all bonds required by the eRFP and described on Exhibit H attached hereto and deliver a true, correct, and complete copy of the same to State.

13.2 Required Coverage. Contractor, at its sole expense, shall obtain and keep in force at all times during the Term insurance coverage for the benefit of Contractor and State, issued by insurance carriers licensed to do business in the State of Georgia with a minimum A.M. Best rating of A- as set forth in Exhibit H as that Exhibit may be updated and modified from time to time by State (provided Contractor is given a reasonable amount of time to review and meet such updated and modified insurance requirements).

13.3 Primary Policies. All insurance maintained by Contractor in compliance with this Agreement, shall be primary to any other insurance owned, secured, or placed on behalf of State, which insurance shall not be called upon by Contractor's insurer to contribute in any way. Contractor shall secure endorsements to this effect from all insurers of such policies.

13.4 Certificates. Within ten (10) days of the Effective Date, Contractor shall furnish State with certificates of insurance and necessary endorsements affecting coverage required by this Section 13. To the maximum extent permitted for each coverage type, the certificates and endorsements shall identify the contract number of this Agreement (as shown on the cover page), the State of Georgia, State, and the other State Entities as additional insureds and shall be signed by a person authorized by that insurer to bind coverage on its behalf. State reserves the right to require complete, certified copies of all required insurance policies, at any time.

13.5 No Cancellation. All policies herein shall expressly provide that such policies shall not be cancelled, allowed to lapse, terminated or materially altered (resulting in failure to comply with requirements set forth herein) without at least thirty (30) days prior written notice to State.

13.6 Waiver. To the extent permitted by its respective policies of insurance, Contractor hereby waives any right of recovery against State for any loss or damage that is covered by any insurance policy maintained or required to be maintained with respect to this Agreement. The parties do not intend to shift all risk of loss to insurance. The Contractor's obligation to maintain insurance coverage in specified amounts will not act as a limitation on any other liability or obligation which the Contractor may otherwise have under this Agreement. Similarly, the inclusion of the State of Georgia and the State Entities as additional insured is not intended to be a limitation of the Contractor's liability under this Agreement and will in no event be deemed to, or serve to, limit the Contractor's liability to the State or any State Entity to required insurance coverage, nor to limit State's rights to exercise any and all remedies available to the State Entities under this Agreement, at law or in equity.

14. REPRESENTATIONS AND WARRANTIES.

14.1 Warranties. Contractor hereby expressly represents, warrants, and covenants to State that:

14.1.1 Organization. It is a corporation duly organized, validly existing, and in good standing under the laws of the State of Delaware, and it is duly qualified to conduct business, and is in good standing, in the State of Georgia and every other jurisdiction in which the nature of its assets or its business would require it to so qualify.

14.1.2 Authority. (a) It has full power and authority to enter into this Agreement, to grant the rights granted hereunder and to perform its obligations under this Agreement; (b) execution and performance of this Agreement shall not violate any law or breach any other agreement known to Contractor; and (c) Contractor will not assume any obligation or restriction that does or would in any way interfere or conflict with, or would prevent, limit, or impair in any way the performance by Contractor of any of the terms of this Agreement or of the Services.

14.1.3 Liens and Encumbrances. Contractor has good and valid title to the Solution and all Equipment or hardware components provided to the State Entities pursuant to the terms of this Agreement free and clear of any and all liens and encumbrances. All such items will be delivered, and title will transfer, to the applicable State Entity pursuant to Section 2.1.5 free and clear of all liens and encumbrances and State will be entitled to use the Solution and all other Deliverables in accordance with the terms of this Agreement without disturbance.

14.1.4 eRFP Bring Down. Each of the representations, warranties, guarantees, certifications, and similar assurances contained in Contractor's eRFP Response were true and correct in all respects as of the date of submission of Contractor's eRFP Response and shall be true and correct in all respects on and as of the Effective Date with the same force and effect as if made at and as of the Effective Date.

14.1.5 Non-Infringement. As of the Effective Date and throughout the Term:

(a) None of the Solution, Services, or other Deliverables, nor any portion or component thereof, nor State's use or possession of any of the foregoing as permitted under this Agreement, shall infringe or violate any right, title, or interest (including any Intellectual Property Right) of any third party.

(b) Contractor and/or all Contractor Personnel shall be the sole authors of the Solution and any Revisions thereto and Contractor has and shall have full and sufficient right, title and interest (including all Intellectual Property Rights) in and to the Solution.

(c) No claim of infringement has been threatened or asserted, or is pending against Contractor (or insofar as Contractor is aware, against any entity from which Contractor has obtained such rights) (the warranties set forth in clauses "(a)", "(b)", and "(c)" collectively the "**Non-Infringement Warranty**").

14.1.6 Disabling Procedures. The Solution, State-Specific Enhancements and other Deliverables and each module or component and function thereof, and to the maximum extent applicable, the Services performed hereunder, do not contain any "back door," "time bomb," "Trojan horse," "drop dead device," or other similar software routines or components designed to permit access or use of any State Entities' computer systems by Contractor or a third party or to disable or delete any Solution or any data, computer hardware, or software operated or maintained by any State Entity;

14.1.7 Viruses. The Licensed Programs, State-Specific Enhancements and other Deliverables and each module or component and function thereof, and to the maximum extent applicable, the Services performed hereunder, do not contain any Virus and prior to delivery to the State Entities, Contractor shall have used up-to-date, industry-accepted, corporate-enterprise, quality virus detection products to scan for and ensure the absence of Viruses. Contractor shall take all commercially reasonable steps to ensure that no Viruses are coded or introduced into any other State Entities' systems or into the systems used to provide the Services or operate the Solution;

14.1.8 EAC Certification. All relevant components of the Solution, any Upgraded Solution, and all Software, Equipment, and other components forming a part thereof for which certification by the U.S. Election Assistance Commission ("**EAC**") is available have been certified by the EAC as of delivery of the Solution to the State. Without limiting the foregoing, if at any time during the Term, the Solution or any component (including Software and Equipment) forming a part thereof for which EAC certification is available ceases to be certified by the EAC, Contractor shall immediately notify State and, if Contractor has, or has made available a non-infringing, EAC certified, version of the offending component to its

customers generally, then Contractor will make that version of the Solution available to the State under the same or better economic terms as it offers to its other customers. If no EAC certified version of the offending component is available, the parties will cooperate in good faith to attempt to resolve the issue.

14.1.9 Documentation. The Documentation meets industry standards, accurately reflects the operations features and functioning of the Solution, Services and Deliverables and shall in all events be written in the English language as well as such other languages as are required under the applicable Solution Order or Services Order.

14.1.10 Services. Contractor has all of the resources (financial or otherwise), personnel, experience, and know-how necessary for the successful and timely implementation of the Solution and performance of its obligations under this Agreement. All Services performed by Contractor (or its permitted subcontractors, if any) shall be so performed in accordance with all Applicable Laws and in a professional and workmanlike manner by adequate staff having the skills training and background requisite to perform them in accordance with the highest prevailing standards and best practices in the industry.

14.1.11 Operations Conducted Lawfully. Contractor has conducted, and at all times during Term will conduct, its business in compliance with all Applicable Laws including with the provisions of O.C.G.A. Title 21, as amended and the State of Georgia Election Board and Secretary of State Rules contained in Sections 183 and Sections 590 of the Georgia Administrative Code respectively. Contractor has not been charged with, nor is Contractor in receipt of any notice or warning of, or to the knowledge of Contractor, under investigation with respect to, any failure or alleged failure to comply with any provision of any Applicable Law with respect to its business, the Solution, or the Services to be provided pursuant to this Agreement. Contractor has all licenses, permits, approvals, authorizations, registrations, certificates, variances or similar rights issued by any governmental authority required with respect to the operation of its business and the delivery of the Solution and the Services. All such permits are in full force and effect and Contractor is in compliance with the same.

14.1.12 Solution and other Deliverables. During the Term the Solution and all Deliverables and each module or component and function thereof, and to the maximum extent applicable, all Services performed hereunder, shall:

- (a) be free from defects in material and workmanship and under normal use shall remain in good working order;
- (b) function in all material respects in accordance with the specifications and criteria stated in the applicable Solution Order or Services Order, including the Functional Requirements, and in accordance with all other warranties set forth herein and in the applicable Solution Order or Services Order (the "**Specifications Warranty**"); and
- (c) perform the Guaranteed Functionality in accordance with the Guaranteed Performance,

14.1.13 Compliance with Regulations. The Guaranteed Functionality and Guaranteed Performance of the Solution, either by itself or in conjunction with such Third Party Materials as may be identified by Contractor, contain features and functionality that permit State, or the applicable State Entity, to comply either through use of the Solution as delivered or via no more than *de minimis* parameterization and/or configuration, with those industry and/or governmental regulations (and the data formats, records, reporting or communications standards required to be utilized to comply with such regulations) affecting State at each State Site as of the Effective Date ("**Regulation Compliant**").

14.1.14 Third Party Materials. If the warranties to Third Party Materials passed-through and assigned to State under Sections 12.7 and 14.2 are not substantially similar to the warranties received by State from Contractor hereunder with respect to the Solution and other Deliverables, or if Contractor is not permitted to pass-through and assign such warranties, then Contractor shall obtain comparable warranties from the owner, licensor, or other providers of the applicable Third Party Materials or Contractor shall take

appropriate action to ensure that such Third Party Materials are otherwise compliant with the warranties in this Section 14.1 including that they are free of Viruses, preventative routines, and disabling procedures.

14.1.15 Independent Contractors. Contractor represents and warrants that it has complied with, and covenants that during the Term, it shall continue to comply with all laws, rules, and regulations required by appropriate government authorities of independent contractors, including the appropriate withholding, reporting, and payment of all required taxes.

14.1.16 Conflicts of Interest. Contractor has not violated, and shall not violate during the Term, the provisions of O.C.G.A. Section 45-10-20 et seq. Without limiting the foregoing, neither Contractor nor any of its Affiliates or any of their respective Representatives has made any bribe, rebate, payoff, influence payment, kickback or other payment unlawful under any Applicable Law.

14.2 Construction of Warranties; Disclaimer. Contractor shall assign and pass through to the State Entities all applicable Software publishers' warranties, covenants and indemnification provisions. The representations, warranties, and covenant of Section 14.1 apply at all times during the Term. EXCEPT FOR THE WARRANTIES SPECIFICALLY PROVIDED IN THIS AGREEMENT (INCLUDING ALL EXHIBITS, SCHEDULES, APPENDICES, EXECUTED SOLUTION ORDERS AND SERVICES ORDERS, AND ANY ATTACHMENTS THERETO) AND AS OTHERWISE SET FORTH ABOVE, CONTRACTOR DISCLAIMS ALL OTHER REPRESENTATIONS AND WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY BASED ON A COURSE OF DEALING, COURSE OF PERFORMANCE OR USAGE OF TRADE.

14.3 Remedies.

14.3.1 Remedies. In the event that any of the Software is found by the Contractor, State, any other State Entity or governmental agency, or any court having jurisdiction to to breach the warranties set forth in this Agreement, or not to be otherwise in compliance with any standard or requirement so as to require or make advisable that such Software be reworked or recalled, the Contractor will promptly communicate all relevant facts to the State Entity and undertake all corrective actions authorized by the State, including those required to meet all obligations imposed by laws, regulations, or orders, provided that nothing contained in this section shall preclude State from taking such action as may be required of it under any such law or regulation. If the Contractor is the Software publisher, the Contractor shall perform all necessary repairs or modifications at its sole expense, provided the State determines the performance of such repairs and modifications is in the State's best interest. Payment for the Software shall not constitute acceptance. Acceptance by a State Entity shall not relieve the Contractor of its warranty or any other obligation under this Agreement.

14.3.2 In the event State or any other State Entity asserts any claim, demand, dispute relating to the subject of this Agreement Contractor shall continue to perform its obligations hereunder, and any such dispute, whether as to a claim for breach of any representation, warranty, or covenant contained in this Agreement, shall not affect Contractor's obligation to fulfill its remedy obligations to the State Entities hereunder. If any such dispute is finally resolved in State's favor, State shall be reimbursed for the cost of all reasonable remediation services performed by Contractor, subject to State substantiating the same.

14.3.3 Disabling Procedures, Preventative Routines and Viruses. In addition to all other remedies at law and under this Agreement, Contractor agrees to notify State immediately upon discovery of any actual, potential or threatened breach of the warranties in Sections 14.1.6 or 14.1.7, and, if State discovers or reasonably suspects any Viruses to be present in any component of any Solution, State-Specific Enhancements or other Deliverables, Contractor agrees to take action immediately, at its own expense, to identify and eradicate (or to equip State to identify and eradicate) such Viruses and carry out any recovery necessary to remedy any impact of such Viruses.

14.3.4 Interference with Services. Contractor is under no obligation or restriction, nor will it assume any such obligation or restriction that does or would in any way interfere or conflict with, or would

prevent, limit, or impair in any way the performance by Contractor of any of the terms of this Agreement or of the Services.

15. INDEMNIFICATION.

15.1 Contractor Indemnification. Contractor agrees to defend, indemnify, and hold harmless State, the other State Entities, and all parties making authorized use of the Deliverables, and each of their respective directors, officers, employees, and representatives (the “**Indemnified Parties**”) from and against any and all liabilities, claims, damages, suits, judgments, losses, costs, and expenses (including reasonable attorneys’ fees) to the extent incurred in connection with or arising out of: (a) any inaccuracy or breach of a representation or warranty of Contractor set forth in this Agreement or any agreement, instrument, or certificate, or document delivered in connection herewith (including Contractor’s eRFP Response); (b) any breach or failure to comply with any covenant or agreement made by Contractor in this Agreement or any agreement or instrument delivered in connection herewith; (c) any negligent, intentional or wrongful act or omission of the Contractor or any Contractor Personnel; (d) any breach of contract; (e) any third-party claims of infringement or other violations of Intellectual Property Rights; (f) any failure of the Solution or the Services to comply with applicable specifications, warranties, and certifications under this Agreement or Contractor’s eRFP Response; (g) any failure by Contractor or Contractor Personnel to comply with Applicable Law; or (h) any failure by the Contractor to make all reports, payments and withholdings required by federal and state law with respect to social security, employee income and other taxes, fees or costs required by the Contractor to conduct business in the State of Georgia or the United States. Contractor acknowledges and agrees that no delay in notifying Contractor shall relieve Contractor of its obligations under this Section 15.1. Contractor may not agree to any settlement that could have an adverse impact on any State Entity, as applicable, without State’s prior written consent. Notwithstanding the foregoing State, and not Contractor, will be responsible and therefore solely liable for its own acts and omissions constituting gross negligence, willful misconduct or fraud.

15.2 Assumption of Defense. State shall be entitled to participate in the defense of any such action, with its counsel and at its own expense. If Contractor does not promptly commence fulfillment of its defense obligations for any indemnified claim or litigation resulting therefrom, State may defend against such claim or litigation in such manner as it may deem appropriate, including settling such claim or litigation, after giving notice of the same to Contractor, on such terms as State may deem appropriate but after prior written consent from Contractor signed by the designated person signing this Agreement, and no action taken by State in accordance with such defense and settlement shall relieve Contractor of its indemnification obligations herein with respect to any loss, liability, or damages resulting therefrom.

15.3 Infringement Related Remedies. In addition to and without in any way limiting or excluding Contractor’s indemnification obligations, if any party makes any claim or allegation of infringement against State or State Entity based on State’s or a State Entity’s use of a Deliverable in accordance with the terms of this Agreement and State or any State Entity is actually enjoined from using any Deliverables (or, if Contractor earlier believes that such claim may arise), Contractor shall, at its own cost and expense, and at its option: (a) procure for State a license to continue using the allegedly or potentially infringing materials of nature and scope identical to that contained in this Agreement and without loss, diminution or degradation in the manner of performance or functionality or (b) modify the allegedly or potentially infringing materials so as to make them non-infringing without loss, diminution or degradation in the manner of performance or functionality. If Contractor cannot complete “(a)” or “(b)” above after good faith efforts undertaken for a reasonable period of time, then Contractor shall, at its own cost and expense: (c) procure for State and the State Entities a license to a third-party product (including, if required, engaging a third-party to develop such product on commercially reasonable terms) that will serve as a replacement for the allegedly or potentially infringing materials without loss, diminution or degradation in the manner of performance or functionality. If Contractor cannot complete “(a),” “(b)” or “(c)” above after good faith efforts undertaken for a reasonable period of time, on commercially reasonable terms, Contractor promptly shall refund to State all amounts paid by State under the Services Order (including any expenses and fees for Third Party Materials) pursuant to which the applicable materials were created.

15.4 Duty to Reimburse State Tort Claims Fund. To the extent any damage or loss as covered by this indemnification is covered by the State of Georgia Tort Claims Fund ("the **Fund**"), the Contractor (and its insurers) agrees to fully reimburse the Fund. To the full extent permitted by the Constitution and the laws of State and the terms of the Fund, the Contractor and its insurers waive any right of subrogation against State, the Indemnified Parties, and the Fund and insurers participating thereunder, to the full extent of this indemnification.

15.5 Limitation of Liability.

15.5.1 EACH PARTY'S TOTAL AGGREGATE LIABILITY FOR ANY LOSS, DAMAGE, COSTS OR EXPENSES UNDER OR IN CONNECTION WITH THIS AGREEMENT, HOWSOEVER ARISING, INCLUDING WITHOUT LIMITATION, LOSS, DAMAGE, COSTS OR EXPENSES CAUSED BY BREACH OF CONTRACT, NEGLIGENCE, STRICT LIABILITY, BREACH OF STATUTORY OR ANY OTHER DUTY SHALL IN NO CIRCUMSTANCES EXCEED THE TOTAL DOLLAR AMOUNT OF THE AGREEMENT, INCLUDING ALL SOLUTION ORDERS AND SERVICES ORDERS IN EFFECT AS OF THE DATE OF THE APPLICABLE CLAIM.

15.5.2 NEITHER PARTY SHALL BE LIABLE FOR ANY LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF USE OR ANY OTHER INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL OR CONSEQUENTIAL LOSS OR DAMAGE WHATSOEVER, HOWSOEVER ARISING, INCURRED BY THE OTHER PARTY OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT, NEGLIGENCE OR OTHER TORT, EVEN IF THE PARTIES OR THEIR REPRESENTATIVES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

15.5.3 Notwithstanding anything contained in this Agreement to the contrary the limitations and exclusions in Sections 15.5.1 and 15.5.2 shall not apply to (1) Contractor's obligation to pay any liquidated damages pursuant to Section 10.1, (2) Contractor's failure to honor any pricing commitments made in this Agreement, (3) claims arising out of the willful misconduct or gross negligence of a Party or any of their respective employees, agents, contractors or subcontractors, (4) claims and losses that are the subject of indemnification under this Agreement, including pursuant to Section 15, (5) damages and costs associated with the Contractor's breach of its data security or data privacy obligations hereunder; (6) damages attributable to a Party's breach of its obligations with respect to Confidential Information of the other Party; or (7) damages attributable to the abandonment of this Agreement by the Contractor, including Termination Assistance, where "abandonment" has the meaning provided in Section 16.8 below.

16. TERM AND TERMINATION.

16.1 Term. This initial term of this Agreement shall commence upon the Effective Date and shall remain in effect for a period of ten (10) years (the "**Initial Term**"). State shall have the option to extend this Agreement for a period of up to ten (10) successive periods of one (1) year each (each a "**Renewal Period**") under the same terms and conditions of this Agreement as in effect during the Initial Term, which options may be exercised by the issuance of a "Notice of Award Amendment" by State no later than thirty (30) days prior to the end of the Initial Term or then-current Renewal Period. As used throughout this Agreement, all references to the "**Term**" shall be construed to include the Initial Term, all Renewal Periods, and any Transition Assistance Period.

16.2 Immediate Termination. Pursuant to O.C.G.A. Section 50-5-64, this Agreement will terminate immediately and absolutely if State determines that adequate funds are de-appropriated such that State cannot fulfill its obligations under the Agreement, which determination is at the State's sole discretion and shall be conclusive.

16.3 Termination for Cause. Subject to Section 16.3.133.13, the State may terminate any Solution Order, Services Order or this Agreement, in each instance in whole or in part, if State reasonably determines that any one or more of the following events has occurred:

16.3.1 The actions, or failure to act, of the Contractor, its agents, employees, or subcontractors have caused, or reasonably could cause, life, health, or safety to be jeopardized;

16.3.2 Contractor fails to comply with confidentiality laws or provisions, including the Privacy Regulations;

16.3.3 Contractor furnished any statement, representation, or certification in connection with this Agreement or the bidding process which is materially false, deceptive, incorrect, or incomplete;

16.3.4 Contractor fails to deliver or has delivered nonconforming goods or services or fails to perform, to State's satisfaction, any material requirement of this Agreement, individually, in each case in whole or in part or is in violation of a material provision of this Agreement, including, but without limitation, the express warranties made by the Contractor;

16.3.5 Satisfactory performance of this Agreement is substantially endangered or that a default is likely to occur, including in connection with Contractor's inability or unwillingness to meet the milestones or timelines described in any Solution Order or Services Order;

16.3.6 Contractor fails to make substantial and timely progress toward performance of this Agreement;

16.3.7 Contractor becomes subject to any bankruptcy or insolvency proceeding under federal or state law to the extent allowed by applicable federal or state law including bankruptcy laws; the Contractor terminates or suspends its business; or State reasonably believes that the Contractor has become insolvent or unable to pay its obligations as they accrue consistent with applicable federal or state law;

16.3.8 Contractor has failed to comply with applicable federal, state and local laws, rules, ordinances, regulations, and orders when performing within the scope of this Agreement;

16.3.9 Contractor has engaged in conduct that has or may expose the State or any State Entity to liability, as determined in State's sole discretion;

16.3.10 Contractor endangers the value, integrity, or security of any State Site or the data or personnel of any State Entity;

16.3.11 Contractor breaches any of its material duties or obligations under this Contractor, including but not limited to obtaining and maintaining, throughout the Term, federal and State voting system certification; or

16.3.12 Contractor has infringed any patent, trademark, copyright, trade dress or any other intellectual property right of State, a State Entity, or any other Person.

16.3.13 Notice of Default. Contractor shall be afforded thirty (30) calendar days to cure any breach that could give rise to a termination for cause by State pursuant to Section 16.3, with such thirty (30) day period commencing as of the date Contractor receives written notice of such breach from the State. If the breach or noncompliance is not remedied within such thirty (30) day period, State may (i) immediately terminate this Agreement without additional written notice; and/or, (ii) procure substitute Software, Licensed Programs or Services from another source and charge the difference between this Agreement and the substitute contract to the defaulting Contractor; and/or (iii) enforce the terms and conditions of this Agreement and seek any legal or equitable remedies. For the avoidance of doubt the parties acknowledge and agree that the items listed in Section 16.3 shall each constitute a material breach, provided, however any reference to specific breaches being material breaches within this Agreement will not be construed to mean that other breaches are not material. If termination occurs prior to the date of Final Acceptance or the Presidential Preference Primary, whichever is later, and such termination is for cause pursuant to Section

16.3, then State may elect to terminate this Agreement and Contractor shall immediately refund all applicable Milestone Payments paid by State.

16.4 Convenience. State may at any time for any reason or no reason, terminate this Agreement or any Solution Order or Services Order individually, in each case in whole or in part, for its sole convenience for any reason whatsoever.

16.5 Effect. Termination of a Solution Order, a Services Order or this Agreement shall not limit either party from pursuing any other remedies available to it, including injunctive relief. Subject to Section 16.6 and Section 16.7 upon termination or expiration of this Agreement and request of the State Entity, the Contractor shall:

16.5.1 Cease work under this Agreement or the applicable Solution Order or Services Order and take all necessary or appropriate steps to limit disbursements and minimize costs, and furnish a report within thirty (30) days of the date of notice of termination, describing the status of all work under the this Agreement, including, without limitation, results accomplished, conclusions resulting therefrom, and any other matters State may require;

16.5.2 Immediately cease using and return to the State Entity any personal property or materials, whether tangible or intangible, provided by the State Entity to the Contractor;

16.5.3 Comply with State's instructions for the timely transfer of any active files and work product produced by the Contractor under this Agreement;

16.5.4 Cooperate in good faith with the State Entity, its employees, agents, and contractors during the transition period between the notification of termination and the substitution of any replacement contractor; and

16.5.5 Immediately return to the State Entity any payments made by the State Entity for goods and services that were not delivered or rendered by the Contractor.

16.5.6 Payment Limitation in Event of Termination. In the event of termination of this Agreement, a Solution Order, or any Service Order for any reason by State, State shall pay only those amounts, if any, due and owing to the Contractor for goods and services actually delivered and satisfactorily performed up to and including the date of such termination. Payment will be made only upon submission of invoices and proper proof of the Contractor's claim. This provision in no way limits the remedies available to the State Entity under the Agreement in the event of termination. State shall not be liable for any costs incurred by the Contractor in its performance of this Agreement, including, but not limited to, startup costs, overhead, or other costs associated with the performance of this Agreement or the bidding process.

16.5.7 In such case, State shall pay for all Services Orders and Solution Orders and Deliverables to the extent delivered and satisfactorily performed by Contractor until the date of such termination. If this Agreement is terminated, Contractor will complete all Services in process under all then-outstanding Solution Orders and Services Orders and adhere to all terms and conditions outlined in this Agreement, including all credits and discounts set forth on the applicable Solution Order or Service Order.

16.6 Transition and Termination Assistance. If State decides to discontinue use of any applications or services, Contractor will, at State's option, provided that State agrees to pay Contractor's reasonable fees and expenses, assist to cause the orderly transition and migration with regard to State's requirements so that State or third-party contractors contractor(s) selected by State are properly equipped to meet those requirements (the "**Termination Assistance**"). As part of the Termination Assistance, (a) Contractor and State will work together to develop a transition plan (the "**Transition Plan**") setting forth the respective tasks to be accomplished by each party in connection with the orderly transition and a schedule pursuant to which the tasks are to be completed and (b) Contractor will provide State with tables and instructions for extraction of data and reports and conducting testing procedures incident to such migration.

16.7 Continuance of Services. Notwithstanding anything contained in this Agreement to the contrary, upon any termination or expiration of this Agreement or any Schedule relating to the provision of applications or services by Contractor, Contractor shall, if requested by State, continue to provide the applications or services and accept additional Solutions Orders and/or Services Orders for up to two (2) years or such longer period as the parties may mutually agree (the “**Transition Assistance Period**”) in the manner described herein and in the applicable Schedule and provide such additional assistance as mutually agreed upon between the parties and as reasonably necessary for State to effect an orderly transition of operational responsibilities for the terminated applications or services. Such termination assistance may include: (a) providing reasonable assistance to State in establishing or transferring all processes; (b) assisting State with the execution of parallel processing and testing; (c) doing all things and providing all information reasonably necessary for an orderly transition with reasonable continuity of operations; and (d) carrying out such other activities as the parties may agree is necessary.

16.8 No Abandonment. Contractor represents, warrants and covenants that, during the Term, it shall not “Abandon” this Agreement (or any Schedule) or application or service obtained by State thereunder. For purposes hereof, “Abandon” or “Abandonment” means the threatened or actual intentional refusal by Contractor to provide or support any of the solutions or perform any of the services in breach of its obligations under this Agreement (or any Schedule). If Contractor breaches or threatens to breach this Section, Contractor agrees that State will be irreparably harmed, and, without any additional findings of irreparable injury or harm or other considerations of public policy, State shall be entitled to apply to a court or tribunal of competent jurisdiction for and, provided State follows the appropriate procedural requirements (e.g., notice), Contractor shall not oppose the granting of an injunction compelling specific performance by Contractor of its obligations under the Agreement without the necessity of posting any bond or other security. Contractor further agrees not to oppose any such application for injunctive relief by State except to require that State establish that Contractor has committed an Abandonment.

17. MISCELLANEOUS.

17.1 Notice. All notices to be given to the parties hereunder shall be in writing and shall be deemed to have been given and be effective when delivered personally or if sent by certified mail, return receipt requested, postage prepaid addressed to the parties at the addresses set forth below.

If to State:

Georgia Secretary of State
2 Martin Luther King Jr. Drive,
West Tower, Atlanta, Georgia 30334
Attention: Chief Operating Officer

with copies to:

Attention: General Counsel

If to Contractor:

Dominion Voting Systems, Inc.
1201 18th Street, Suite 210
Denver, CO 80220

Attention: General Counsel

17.2 No Exclusivity. Unless expressly provide in a Solutions or Services Order, State has the right, at any time and without any notice or duty to account to Contractor, to have services performed by State’s own employees or those of other State Entities or, subject to the terms and conditions of this Agreement, to purchase any equipment or services from any other individual or entity, subject at all times to its compliance with this Agreement. Nothing contained in this Agreement shall constitute a minimum purchase commitment by State, and Contractor has not relied on any representation, verbal or written, to the contrary.

17.3 Language. The headings as to the contents of particular sections of this Agreement are inserted for convenience of reference only and shall in no way define, limit, expand, or otherwise affect the construction or interpretation of any provision of this Agreement. The language of all parts of this Agreement shall in all cases be construed as a whole according to its fair meaning and not strictly for or against either of the parties. Those terms, acronyms, and phrases used but not otherwise defined in this Agreement, which are utilized in the information technology outsourcing industry or in State's contracting processes will be interpreted in accordance with their generally understood meaning in such industry or context.

17.4 Governing Law. This Agreement shall be interpreted and construed under the laws of the State of Georgia, USA, without regard to its conflicts of law principles. The United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Agreement or any services or products provided hereunder. Any judicial action or proceeding between the parties relating to this Agreement must be brought in the courts of Fulton County, Georgia or the United States District Court for the Northern District of Georgia. Each party consents to the jurisdiction of such courts, agrees to accept service of process by mail to the addresses outlined in Section 17.1 (Notice) above, and hereby waives all jurisdictional and venue defenses otherwise available to it.

17.5 Parties' Duty to Provide Notice of Intent to Litigate and Right to Demand Mediation. In addition to any dispute resolution procedures otherwise required under this Agreement or any informal negotiations which may occur between State and the Contractor, no civil action with respect to any dispute, claim or controversy arising out of or relating to this Agreement may be commenced without first giving fourteen (14) calendar days written notice to State of the claim and the intent to initiate a civil action. At any time prior to the commencement of a civil action, either the State or the Contractor may elect to submit the matter for mediation. Either State or the Contractor may exercise the right to submit the matter for mediation by providing the other party with a written demand for mediation setting forth the subject of the dispute. The parties will cooperate with one another in selecting a mediator and in scheduling the mediation proceedings. Venue for the mediation will be in Atlanta, Georgia; provided, however, that any or all mediation proceedings may be conducted by teleconference with the consent of the mediator. The parties covenant that they will participate in the mediation in good faith, and that they will share equally in its costs; provided, however, that the cost to State shall not exceed five thousand dollars (\$5,000.00). All offers, promises, conduct, and statements, whether oral or written, made in the course of the mediation by any of the parties, their agents, employees, experts, and attorneys, and by the mediator or employees of any mediation service, are inadmissible for any purpose (including but not limited to impeachment) in any litigation or other proceeding involving the parties, provided that evidence that is otherwise admissible or discoverable shall not be rendered inadmissible or non-discoverable as a result of its use in the mediation. Inadmissibility notwithstanding, all written documents shall nevertheless be subject to the Georgia Open Records Act O.C.G.A. Section 50-18-70 et seq. No party may commence a civil action with respect to the matters submitted to mediation until after the completion of the initial mediation session, forty-five (45) calendar days after the date of filing the written request for mediation with the mediator or mediation service, or sixty (60) calendar days after the delivery of the written demand for mediation, whichever occurs first. Mediation may continue after the commencement of a civil action, if the parties so desire.

17.6 Assignment.

17.6.1 This Agreement shall not be assignable by either party without the prior written consent of the other party. Notwithstanding anything contained herein to the contrary, State may assign to any other State Entity, in whole or in part, State's right, title, interest and obligations under this Agreement or any Solutions Order or Services Order which relate to items purchased by State on behalf of such State Entity, without Contractor's consent. State's assignment pursuant to this Section 17.6.1 of any payment obligations to another State Entity shall be limited to the extent of that State Entity's interest or use of the subject matter hereof and shall constitute a full and complete novation of State's liabilities and obligations with respect thereto and Contractor shall recognize the State Entity to which such obligations were assigned as State's successor-in-interest with respect to such obligations and will exclusively look to such State Entity for the discharge of all such liabilities and obligations, provided, however State will continue to be Contractor's sole point of contact with respect to this Agreement in accordance with Section 17.234.

17.6.2 This Agreement shall be binding upon and shall inure to the benefit of and be enforceable by the parties hereto and their respective permitted successors and assigns, provided that no assignment, except as described in Section 17.6.1, shall relieve any party of such party's obligations hereunder without the consent of the other party hereto.

17.7 Covenant Against Pledging. Contractor agrees that, without the prior written consent of State, it will not assign, transfer, pledge, hypothecate or otherwise encumber its rights to receive payments from any State Entity under this Agreement for any reason whatsoever. To the extent State permits Contractor to assign, transfer, pledge, hypothecate or otherwise encumber its rights to receive payments from State under this Agreement, Contractor will continue to be State's sole point of contact with respect to this Agreement, including with respect to payment. The Person to which such rights are assigned, transferred, pledged, hypothecated or otherwise encumbered will not be considered a third party beneficiary under this Agreement and will not have any rights or causes of action against any State Entity.

17.8 No Liens. Contractor will not file, or by its action or inaction permit, any liens to be filed on or against property or realty of State or any other State Entity. In the event that any such liens arise as a result of the Contractor's action or inaction, Contractor will obtain a bond to fully satisfy such liens or otherwise remove such liens at its sole cost and expense within ten (10) Business Days. If Contractor fails to do so, State may, in its sole discretion, pay the amount of such lien, or deduct such amounts from payments due to Contractor.

17.9 Non-Delegation. Nothing herein will be deemed or construed as delegating the discretionary powers or authority of State or any of the other State Entities to Contractor. Further, nothing herein will be deemed or construed as delegating the discretionary powers or authority of the other State Entities to State or the discretionary powers or authority of State to the other State Entities.

17.10 No Waiver. The failure of either party at any time or times to enforce or require performance of any provision contained in this Agreement shall in no way operate as a waiver or affect the right of such party at a later time to enforce such provision.

17.11 Entire Agreement. This Agreement (together with its Exhibits, all executed Solution Orders and Services Orders, and all attachments thereto) constitutes the entire agreement between the parties hereto with respect to the subject matter hereof. This Agreement supersedes all prior written agreements and contemporaneous oral agreements with respect to the subject matter hereof; provided, if the parties have entered into a Confidentiality and Non-Disclosure Agreement, the terms of such agreement shall survive and govern the parties' obligations as set forth in such agreement between the execution date thereof and the Effective Date. Although State may utilize its own purchase order or confirmation form for its own convenience, the provisions of this Agreement shall control as to all issues relating to the subject matter hereof. Typewritten or handwritten additions, initialed by both parties, shall supersede any pre-printed provisions of this Agreement. Subject to the foregoing, each Solution Orders and Services Orders hereto, whether executed concurrently herewith or subsequent hereto, shall be deemed to be incorporated herein and shall be governed by the terms of this Agreement.

17.12 Amendment. This Agreement may be amended in writing from time to time by mutual consent of the parties. If the contract award exceeds the delegated purchasing authority of State, then State must obtain approval of the amendment from the Department of Administrative Services (DOAS). All amendments to this Agreement must be in writing and fully executed by duly authorized representatives of State and the Contractor.

17.13 Severability. Each provision herein shall be treated as a separate and independent clause, and the unenforceability of any one clause shall in no way impair the enforceability of any of the other clauses of the Agreement. Moreover, if any provision contained in this Agreement shall for any reason be held to be excessively broad as to scope, activity, subject, or otherwise unenforceable, such provision shall be construed by the appropriate judicial body by limiting or reducing it or them so as to be enforceable to the maximum extent compatible with the Applicable Law.

17.14 Time is of the Essence. Time is of the essence with respect to Contractor's performance of the terms of this Agreement. Contractor shall ensure that all personnel providing Software, Licenses and Services to State are responsive to State's requirements and requests in all respects.

17.15 Independent Contractor. Contractor and all Contractor Personnel are independent contractors and neither Contractor nor any Contractor Personnel shall be deemed an employee of State. Contractor is and shall remain the employer of all Contractor Personnel and shall be solely responsible for the employment, training, and payment of salaries, wages, bonuses, benefits (including health insurance, retirement and other similar benefits, if any) and other compensation, of all Contractor Personnel. Contractor shall be responsible for the payment of all federal, state, and local withholding taxes and workers compensation, and, at the reasonable request of State, Contractor shall provide to State evidence that all of such payments have been made. Nothing in this Agreement shall be construed to create a partnership, joint venture, or agency relationship between the parties. Neither Contractor nor any Contractor Personnel shall have the right to bind State to any contract, agreement, or obligation.

17.16 Joint/Several Liability. If the Contractor is a joint entity, consisting of more than one Person, all such Persons shall be jointly and severally liable for carrying out the activities and obligations of this Agreement, and for any default of activities and obligations. Contractor acknowledges and agrees that that the liability of each State Entity shall be several and not joint.

17.17 No Third-Party Beneficiaries. Nothing expressed or implied in this Agreement is intended or shall be construed to confer upon or give any person other than Contractor and State any rights or remedies under or by reason of this Agreement.

17.18 Survival. All provisions of this Agreement that, by their terms, are intended to survive shall expressly survive any termination or expiration of this Agreement, including Section 3, Section 11, Section 12, Section 14 and Section 15.

17.19 Publicity. The laws of the State of Georgia, including the Georgia Open Records Act, as provided in O.C.G.A. Section 50-18-70 et seq., require procurement records and other records to be made public unless otherwise provided by law. Notwithstanding the foregoing, the Contractor Parties each agree that no acknowledgment or other information concerning the Agreement or the Services and/or Deliverables provided hereunder will be made public by the Contractor Parties without the prior written agreement of State. Further, the Contractor Parties shall not use State's, any other State Entities' name, photographs, logo, trademark, or other identifying characteristics without the applicable State Entity's prior written approval.

17.20 Solicitation. The Contractor warrants that no person or selling agency (except bona fide employees or selling agents maintained for the purpose of securing business) has been employed or retained to solicit and secure this Agreement upon an agreement or understanding for commission, percentage, brokerage or contingency.

17.21 Interpretation; Intent of References to Bid Documents. Whenever any provision of this Agreement uses the term "including" (or "includes"), such term shall be deemed to mean "including without limitation" and "including but not limited to" (or "includes without limitations" and "includes but is not limited to") regardless of whether the words "without limitation" or "but not limited to" actually follow the term "including" (or "includes"). The words "herein," "hereby," "hereunder," "hereof," and other equivalent words shall refer to this Agreement in its entirety and not solely to the particular portion of this Agreement in which any such word is used. All definitions set forth herein shall be deemed applicable whether the words defined are used herein in the singular or the plural. Wherever used herein, any pronoun or pronouns shall be deemed to include both the singular and plural and to cover all genders. The references to the parties' obligations, which are contained in this Agreement, are intended to supplement or clarify the obligations as stated in the eRFP and Contractor's eRFP Response. The failure of the parties to make reference to the terms of the eRFP or Contractor's eRFP Response in this Agreement shall not be construed as creating a conflict and will not relieve the Contractor of the contractual obligations imposed by the terms of the eRFP and the

Contractor's eRFP Response. The contractual obligations of any State Entity cannot be implied from Contractor's eRFP Response.

17.22 Force Majeure. Neither party shall be liable for, or be in breach of this Agreement because of, any delay or failure to perform its obligations under this Agreement or thereunder resulting from any acts of God, war, insurrection, terrorism or the public enemy (collectively, "**FM Events**"). A party that experiences a FM Event shall give the other party prompt written notice of the FM Event. The affected party shall use reasonable efforts to work around or to overcome the FM Event and to resume full performance under this Agreement as soon as practicable. Occurrence of FM Events will not excuse the backup and disaster recovery obligations of Contractor. Contractor will follow normal procedures for classification, resolution, resolution and escalation of incidents, even if the incident is caused by an FM Event. If an FM Event causes a material failure or delay in the performance of any applications or services for more than five (5) consecutive days, State may, at its option, and in addition to any other rights State may have, procure such applications or services from an alternate source until Contractor is again able to provide them, and Contractor shall be liable for all payments made and costs incurred by State required to obtain such applications and services from such alternate source during such period. If an FM Event causes a material failure or delay in the performance of any application or services for more than thirty (30) consecutive days, State may, at its option, and in addition to any other rights they may have, immediately terminate each affected Schedule and Services Order without liability to Contractor. State shall not be required to pay the fees that may have otherwise been payable for any period of time in which any substantial part of the Solution and Services are not provided as a result of an FM Event.

17.23 Counterparts. This Agreement may be executed in any number of separate counterparts, each of which shall collectively and separately constitute one Agreement. Counterparts may be delivered via facsimile, electronic mail (including pdf or any electronic signature complying with the U.S. federal ESIGN Act of 2000, e.g., www.docuSign.com) or other transmission method and any counterpart so delivered shall be deemed to have been duly and validly delivered and be valid and effective for all purposes.

17.24 State Entity Representative. Notwithstanding anything contained in this Agreement to the contrary, each of the State Entities other than State hereby appoint State to serve as their representative and State accepts such appointment, to act for and on behalf of such State Entities with respect to this Agreement. Each of the State Entities acknowledges and agrees that any decision, act, consent, or instruction taken or given by State pursuant to this Agreement shall be and constitute a decision, act, consent or instruction of all State Entities and shall be final, binding, and conclusive upon the State Entities, and Contractor and its Affiliates may rely upon any such decision, act, consent or instruction of State on behalf of the other State Entities. The State Entities hereby agree to release State from and waive any and all claims and liabilities based on any claim that an action authorized hereunder to be taken by the State on behalf of the other State Entities is not binding on, or enforceable against, any such State Entity.

17.25 Order of Precedence. In the case of any inconsistency or conflict among the specific provisions of this Agreement (as amended), the Exhibits attached hereto, the eRFP (including any subsequent addenda), Contractor's eRFP Response, and the Documentation, the order of precedence shall be, notwithstanding any terms that may be contained in the eRFP, Contractor's eRFP Response, or the Documentation (including any statement that purports to change the order of precedence described herein, incorporate additional or inconsistent terms, or amend documents having precedence), as follows:

17.25.1 First, by giving precedence to the specific provisions of this Agreement.

17.25.2 Second, by giving precedence to the specific provisions of the Exhibits attached hereto.

17.25.3 Third, by giving precedence to the specific provisions of the eRFP.

17.25.4 Fourth, by giving precedence to the specific provisions of the Contractor's eRFP Response, except that objections or amendments by a Contractor contained in Contractor's eRFP Response that have not been expressly accepted by State in writing shall not be included in this Agreement and shall be given no weight or consideration.

18. **DEFINITIONS AND INDEX OF PREVIOUSLY DEFINED TERMS.**

This Section 18 provides definitions for capitalized terms used but not previously defined in this Agreement and indexes capitalized terms used and previously defined in the Section in which they first appear as indicated by bold type. The definitions in this Section apply to such capitalized terms in both their singular and plural forms. This Section 18 does not apply to those terms capitalized only to comply with grammatical conventions.

18.1 **“Abandon”** and **“Abandonment”** have the meanings set forth in Section 16.8.

18.2 **“Acceptance Test”** is defined in Section 9.

18.3 **“Acceptance Test Plan”** is defined in Section 9.

18.4 **“Agreement”** is defined in the Initial Paragraph of this Agreement.

18.5 **“Applicable Law”** means all applicable provisions of any constitution, statute, common law, ordinance, code, rule, regulation, decision, order, decree, judgment, release, license, permit, stipulation or other official pronouncement enacted or issued by any Governmental Authority or arbitrator or arbitration panel.

18.6 **“Application Programs”** is defined in Section 2.1.1(ii).

18.7 **“Authorized Recipients”** means those employees, consultants or agents of the Receiving Party to whom disclosure is required to carry out this Agreement and any Order hereunder and who have executed a confidentiality agreement or are otherwise bound to duties of non-disclosure and restrictions on use of the Confidential Information at least as restrictive as those set forth in this Agreement (including, but not limited to an undertaking to implement and maintain appropriate administrative, technical and physical safeguards to protect the confidentiality, integrity and availability of Regulated Information) but shall expressly exclude such individuals or entities as may, at the election of the parties, be identified on a list bearing the signatures of the parties and attached to and incorporated into this Agreement.

18.8 **“Bankruptcy Code”** is defined in Section 3.1.4.

18.9 **“Breach Incident”** is defined in Section 7.2.2(b).

18.10 **“Change Control Form”** is defined in Section 5.2.

18.11 **“Change Order”** is defined in Section 5.2.

18.12 **“Change Request”** is defined in Section 5.2.

18.13 **“Change Response”** is defined in Section 5.2.

18.14 **“Confidential Information”** is defined in Section 11.1.

18.15 **“Configuration Services”** means the services described in Section 4.1.

18.16 **“Contractor”** is defined in the initial paragraph of this Agreement.

18.17 **“Contractor Affiliates”** means those entities that are: (a) directly or indirectly, through one or more intermediaries, controlled by Contractor, whether such control is effective by ownership of equity interests, contract or otherwise; and (b) expressly identified by Contractor to State and State agrees to their inclusion on Exhibit D.

18.18 **“Contractor Computer Systems”** is defined in Section 11.7.1.

18.19 **“Contractor’s eRFP Response”** means Contractor’s submission in response to the eRFP including all materials submitted in connection therewith and, for the avoidance of doubt, all responses to the Mandatory Response Worksheet, questionnaires, and other attachments or links released with the eRFP, a copy of which is attached hereto as Exhibit A.

18.20 **“Contractor Licensed Programs”** means those Licensed Programs identified on the applicable Solution Order as being licensed by Contractor.

18.21 **“Contractor Parties”** is defined in Section 7.3.2.

18.22 **“Contractor Personnel”** is defined in Section 6.2.

18.23 **“Contractor Products”** is defined in Section 12.1.

18.24 **“Contractor Relationship Manager”** is defined in Section 6.1.

18.25 **“Contractor Solution Partner”** is defined in Section 1.3.

18.26 **“Contractor System Proposal”** is defined in Section 4.1.2.

18.27 **“County”** means the 159 counties of the State of Georgia.

18.28 **“Crisis”** means an extraordinary event affecting Contractor that requires emergency response measures to be taken, including any event that may result in the Solution or Services and any additional applications provided by Contractor to State becoming unavailable for a significant amount of time

18.29 **“Critical Milestone”** means those critical delivery and implementation milestones specifically identified in Table A of Appendix A to Attachment 4 of Solution Order No. 1 (Milestones).

18.30 **“Deliverables”** is defined in Section 12.7.

18.31 **“Delivery & Acceptance Notice”** means a written notice substantially in the form of Exhibit I.

18.32 **“Derivative Works & Improvements”** has, collectively, the meaning ascribed to the term “derivative work” in Title 17 U.S.C., and “improvement” in Title 35 U.S.C., but in all events shall apply to additions, changes, or other statutorily specified new material appearing for the first time in the applicable item or work hereunder.

18.33 **“Designated Licensed Programs”** is defined in Section 4.1.1.

18.34 **“Disabling Procedures”** means any program routine, device, code or instructions (including any code or instructions provided by third parties) or other undisclosed feature, including a time bomb, virus, software lock, drop-dead device, malicious logic, worm, Trojan horse, bug, error, defect or trap door, that is capable of accessing, modifying, deleting, damaging, disabling, deactivating, interfering with, or otherwise harming the Services and Deliverables, any hardware, data or other electronically stored information, or computer programs or systems.

18.35 **“Disaster Recovery Plan”** is defined in Section 11.8.

18.36 **“Disclosing Party”** is defined in Section 11.1.

18.37 **“Discounts”** shall mean the discounts set forth in the Fee Schedule.

18.38 **“Documentation”** means all written materials related to any Services or Deliverables (including any component of any Solution) that are supplied by Contractor to State hereunder, including any and all installer's, operator's and user's manuals, training materials, guides, functional and/or technical specifications, commentary, listings and other materials, (including all materials describing interoperability with other hardware or software), in any or all media, for use in conjunction with the applicable Services or Deliverables (including any component of any Solution), in all cases in sufficient form and content to allow for first and frontline personnel comprehension thereof. If such Deliverables are discrete computer software applications, Documentation shall include such reasonable descriptions as would allow a third party of reasonable skill and experience in information technology to operate, maintain, customize and parameterize such Deliverables and their related Source Code.

18.39 **“Effective Date”** is defined in the initial paragraph of this Agreement.

18.40 **“Equipment”** is defined in Section 2.1.1(iv).

18.41 **“Equipment Charge”** is defined in Section 10.1.8.

18.42 **“Extended Warranty”** is defined in Section 4.2.

18.43 **“eRFP”** is defined in Section 1.1.

18.44 **“Fee Schedule”** is defined in Section 10.1.

18.45 **“Final Acceptance”** means the receipt by Contractor of written notification from State that all Services and Deliverables under a given Services Order have been reviewed and tested by State as a whole and found to: (a) substantially conform to the Specifications and descriptions set forth in such Services Order and any exhibits thereto, as such Specifications and descriptions may be specifically amended by subsequent mutual written agreements between the parties; and (b) conform to Contractor's representations and warranties in this Agreement.

18.46 **“FM Events”** is defined in Section 17.22.

18.47 **“Functional Requirements”** is defined in Section 4.1.1.

18.48 **“Fund”** is defined in Section 15.3.

18.49 **“Generally Accepted Accounting Principles”** means United States generally accepted accounting principles.

18.50 **“Governmental Authority”** means any federal, state, local or foreign legislative, executive, judicial, quasi-judicial or other public authority, agency, department, bureau, division, unit, court or other public body.

18.51 **“Guaranteed Functionality”** is defined in Section 1.2.

18.52 **“Guaranteed Performance”** is defined in Section 1.2.

18.53 **“Impact Analysis”** is defined in Section 5.3.

18.54 **“Indemnified Parties”** is defined in Section 15.1.

18.55 **“Initial Acceptance”** means the receipt by Contractor of written notification from State that any particular Services or Deliverables under a given Services Order have been reviewed and/or tested by State and found to: (i) substantially conform to the Specifications and descriptions set forth in such Services Order and any exhibits thereto, as such Specifications and descriptions may be specifically amended by

subsequent mutual written agreements between the parties and (ii) conform to Contractor's representations and warranties in this Agreement.

18.56 **"Initial Term"** is defined in Section 16.1.

18.57 **"Installation Deadline"** is defined in Section 2.1.3.

18.58 **"Installation Event"** is defined in Section 2.1.3.

18.59 **"Installation Plan"** is defined in Section 2.1.3.

18.60 **"Intellectual Property Rights"** means all right, title and interest, including all copyright rights, patent rights (including rights under all patent applications, patents, letters patent, supplementary patent certificates, inventor's certificates, continued prosecution applications, requests for continued examination, and other similar filings or stages thereof) and trademark rights as well as all proprietary rights (including Trade Secrets) and moral rights (including the rights of authorship and attribution and subsequent modification) throughout the world whether under the laws of the United States, any of its several states or any foreign jurisdiction and whether or not evidenced by certificates, applications or registrations therefor and whether granted permanently, on initial issuance or granted upon reissue, re-examination, division, extension, provisionally, in continuation or in continuation-in-part and at all times further including all goodwill associated with all such rights.

18.61 **"Interest Rate"** means the lesser of eighteen percent (18%) or the maximum rate permitted by Applicable Law.

18.62 **"Interruption"** means any material, or continuing, or repeated suspension or interruption in the supply of the Solution or Services by or on behalf of Contractor to State, or any other material, or continuing, or repeated failure of Contractor to meet its obligations under this Agreement in regard to the Solution or Services, whether resulting from breach, termination, partial or complete cessation of business, disruption of business, bankruptcy or other insolvency proceedings, or otherwise, or termination of this Agreement.

18.63 **"Key Personnel"** is defined in Section 6.5.

18.64 **"Licensed Programs"** means all operating system software and other software programs (including all Contractor Licensed Programs and Third Party Licensed Programs) provided by Contractor hereunder.

18.65 **"Major Revisions"** is defined in Section 2.3.

18.66 **"Maintenance Services"** is defined in Sections 2.1.1(v).

18.67 **"Mandatory Requirements"** is defined in Section 1.2.

18.68 **"Milestone Payment"** is defined in Section **Error! Reference source not found.**

18.69 **"Milestone Deadline"** means each of the dates listed in the "Milestone Deadline" column of the tables set forth on Appendix A to Attachment 4 of Solution Order No. 1 (Milestones).

18.70 **"Non-Infringement Warranty"** is defined in Section 14.1.5(c).

18.71 **"Operating Program"** is defined in Section 2.1.1(iv).

18.72 **"OSS"** is defined in Section 12.9.

18.73 **"Output"** is defined in Section 12.1.

18.74 **“Performance Levels”** is defined in Section 8.1.

18.75 **“Performance Requirements”** is defined in Section 4.1.1.

18.76 **“Person”** means any individual, corporation, limited liability company, partnership, limited partnership, business trust, or other entity of any nature.

18.77 **“Pilot Election”** means the pilot election to be administered on November 5, 2019 in up to 6 Counties (exact Counties to be determined by mutual agreement), including the coding of election database (and additional training needed in connection therewith), training of personnel including poll-workers of the Counties hosting the Pilot Election, logic and accuracy testing at each of the participating State Sites, election day support at the participating State Sites, and post-Pilot Election auditing and validation of results.

18.78 **“Privacy Regulations”** is defined in Section 11.5.

18.79 **“Project Manager”** is defined in Section 6.4.

18.80 **“Proprietary Materials”** means: (a) all runtime and non-runtime machine-readable, executable object code, human readable source code, in any language whatsoever (including HTML, CGI, XML, Java, Visual Basic and C) and on any operating or database platform, system or environment whatsoever (including Windows, Unix, Linux, DB2, J2EE, Oracle, SQL or any mainframe) as well as all computer system designs, user interfaces, commented source code, explanations, flow charts, schematics, algorithms, subroutine descriptions, class and object descriptions, memory and overlay maps, statements of principles of operations, architecture standards, data flow descriptions, class, base-class and sub-class descriptions, data structures, control logic and other computer formatting, programming or scripting code; (b) all inventions and discoveries, whether or not patentable, reduced to practice or recorded in a medium; (c) all published and unpublished works of authorship including audio-visual works, "look and feel," artwork, illustrations, images, photographs and printed or graphic matter; (d) all tangible materials, including all prototypes, models, designs, files, templates libraries (.dll or otherwise), tools, graphics, screen displays and/or their other user interface components or "look and feel" (as that phrase is understood and applied under Title 17 U.S.C.), creative content, algorithms, formulae data, information, reports and technologies; (e) business and technical requirements and system designs and architectures in any form or medium.

18.81 **“Receiving Party”** is defined in Section 11.1.

18.82 **“Regulated Information”** is defined in Section 11.5.

18.83 **“Regulation Compliant”** is defined in Section 14.1.13.

18.84 **“Renewal Period”** is defined in Section 16.1.

18.85 **“Residuals”** means any information in intangible form that is not protectable under copyright or patent law, or protected as a trade secret or other intellectual property right including any ideas, concepts, know-how or techniques contained therein.

18.86 **“Revision”** is defined in Section 2.3.

18.87 **“Security Breach”** means (i) unauthorized physical or technical access to any Contractor Computer System; (ii) any circumstance that may constitute or result in, any unlawful or unauthorized acquisition, access, loss, theft, use or disclosure of any Confidential Information, Regulated Information, or State Data in the possession of any of the Contractor Parties; (iii) any breach or attempted breach of the security of any Confidential Information, Regulated Information, or State Data, or of any of the controls of any of the Contractor Parties intended to protect the same; or (iv) any other circumstances or events that

could compromise the privacy or security of any of the Confidential Information, Regulated Information, or State Data in the possession of any of the Contractor Parties.

18.88 **“Service Level Agreements”** means the service levels to be maintained by Contractor throughout the Term as more fully described in a Services Order or Services Order Attachment.

18.89 **“Services”** is defined in Section 2.1.1.

18.90 **“Services Order”** means a written instrument signed by an authorized signatory of a State Entity and an authorized representative of Contractor substantially in the form of Exhibit C. Such Services Order will include any requirements, considerations, or objectives which differ from the general provisions of this Agreement and not otherwise address in a Solution Order; for example, the intent of the parties with respect to any rights to particular developments (intellectual property), specific Milestone Events and/or Milestone Dates and/or quality and warranty considerations, special fees, and all such other particular objectives, considerations, or requirements in conjunction with the delivery of Services by Contractor. Except as otherwise specifically provided in such Services Order, each Services Order shall be governed by the terms of this Agreement.

18.91 **“Services Order Attachment”** is defined in Section 4.4.

18.92 **“Site Specifications”** means the reasonable environmental specifications as relate to utilities, temperature, and humidity conditions, which Contractor suggests are maintained at the State Sites for efficient operation and use of the Solution at those State Sites.

18.93 **“Software”** is defined in Section 2.1.1.

18.94 **“Solution”** is defined in Section 1.1.

18.95 **“Solution Order”** is defined in Section 2.1.1.

18.96 **“Source Code”** means a copy of the complete source code corresponding to the object code of a given Deliverable, as applicable, plus any pertinent commentary or explanation (including any and all explanations, flow charts, schematics, algorithms, subroutine descriptions, class and object descriptions, memory and overlay maps, statements of principles of operations, architecture standards, data flow descriptions, class, base-class and sub-class descriptions, data structures, and control logic) that may be necessary to render such source code understandable and useable by a reasonably trained computer-programming expert who is generally familiar with information technology systems in the financial and banking sectors. The source code shall include all Documentation, statements of principles of operation, and schematics, all as necessary or useful for the effective understanding and use of such source code. Insofar as the development environment employed for the development, maintenance, and implementation of any source code includes any device, programming, or Documentation not commercially available to State on reasonable terms through readily known sources other than Contractor, the source code shall include all such devices, programming, or Documentation. The foregoing reference to "development environment" is intended to apply to any programs, including compilers, "workbenches," tools, and higher-level (or "proprietary") languages, used by Contractor for the development, maintenance, and implementation of the applicable source code.

18.97 **“Special Programs”** is defined in Section 2.1.1(ii).

18.98 **“Specifications”** means the technical and business requirements of State described in a given Solution Order or Services Order, including all technical detail and design specifications, functionality matrices, requirements definition, request for proposals, proposals, gap analysis, requirements for project management, relevant project considerations, objectives, Milestone Events and/or Milestone Dates, and Performance Levels set forth therein.

18.99 **“Specifications Warranty”** is defined in Section 14.1.12(b).

18.100 **“State”** is defined in the initial paragraph of this Agreement.

18.101 **“State Contractor”** means any individual, corporation, limited liability company, partnership, limited partnership, business trust or other business organization duly recognized under the laws of its applicable jurisdiction that provides services to State or any other State Entity.

18.102 **“State Data”** is defined in Section 12.3.

18.103 **“State Entity”** means the State and the Counties.

18.104 **“State Relationship Managers”** is defined in Section 6.1.

18.105 **“State Site”** means the 159 locations of the State Entities at which the Solution is to be implemented and such other locations as may be designated by State from time to time.

18.106 **“Support Services”** is defined in Section 2.1.1(iii).

18.107 **“SVS”** is defined in Section 1.1.

18.108 [Reserved].

18.109 **“Term”** is defined in Section 16.1.

18.110 **“Termination Assistance”** is defined in Section 15.6.

18.111 **“Termination Assistance Period”** is defined in Section 16.7.

18.112 **“Third Party Licensed Programs”** means those Licensed Programs identified on the applicable Solution Order as being licensed by a Contractor Solution Partner.

18.113 **“Third Party Materials”** means all Proprietary Materials the Intellectual Property Rights for which are owned, by an individual or entity other than State Entities) and Contractor (including Contractor Affiliates).

18.114 **“Trade Secrets”** means any business, scientific or technical data, information, design, process, procedure, formula, or improvement that is commercially valuable to either party and is not generally known in the industry. Each party acknowledges that the Trade Secrets of the other party have been developed by that party at great expense and with the considerable effort of skilled professionals. Each party also acknowledges that the Services and Deliverables under this Agreement may of necessity incorporate Trade Secrets.

18.115 **“Training Services”** is defined in Section 4.2.


18.116 **“Transfer Control Laws”** is defined in Section 7.3.2.

18.117 **“Transition Plan”** is defined in Section 16.6.

18.118 **“Upgraded Solution”** is defined in Section 2.3.

[This space intentionally left blank; signatures appear on following pages.]

IN WITNESS WHEREOF, the parties have caused this Master Solution Purchase and Services Agreement to be executed by their duly authorized representatives as of the date first written above.

STATE OF GEORGIA OFFICE OF THE SECRETARY OF STATE	Dominion Voting Systems, Inc.
By: _____	By:  _____
Name: _____	Name: <u>John Poulos</u>
Title: _____	Title: <u>President & CEO</u>
Date: _____	Date: <u>7/29/2019</u>
By: _____	
Name: _____	
Title: _____	
Date: _____	

RETRIEVED FROM DEMOCRACYDOCKET.COM

EXHIBIT A

To Master Solution Purchase and Services Agreement

CONTRACTOR'S ERF P RESPONSE

RETRIEVED FROM DEMOCRACYDOCKET.COM

EXHIBIT B

To Master Solution Purchase and Services Agreement

SOLUTION ORDER

THIS SOLUTION ORDER is dated this _____ day of _____, 20__ (“**Solution Order Effective Date**”) and is subject to the terms of the Master Solution Purchase and Services Agreement (the “**Agreement**”) dated as of _____, 20109 by and between _____ (“**State**”) and _____ (“**Contractor**”). Unless otherwise defined herein, all capitalized terms used herein have the same meanings as is set forth in the Agreement, which is hereby incorporated by reference. The undersigned State Entity hereby orders delivery for the following pieces of Solution from Contractor. Contractor agrees to deliver the items ordered herein in accordance with the Agreement and in compliance with all Applicable Laws including with the provisions of O.C.G.A. Title 21, as amended and the State of Georgia Election Board and Secretary of State Rules contained in Sections 183 and Sections 590 of the Georgia Administrative Code respectively.

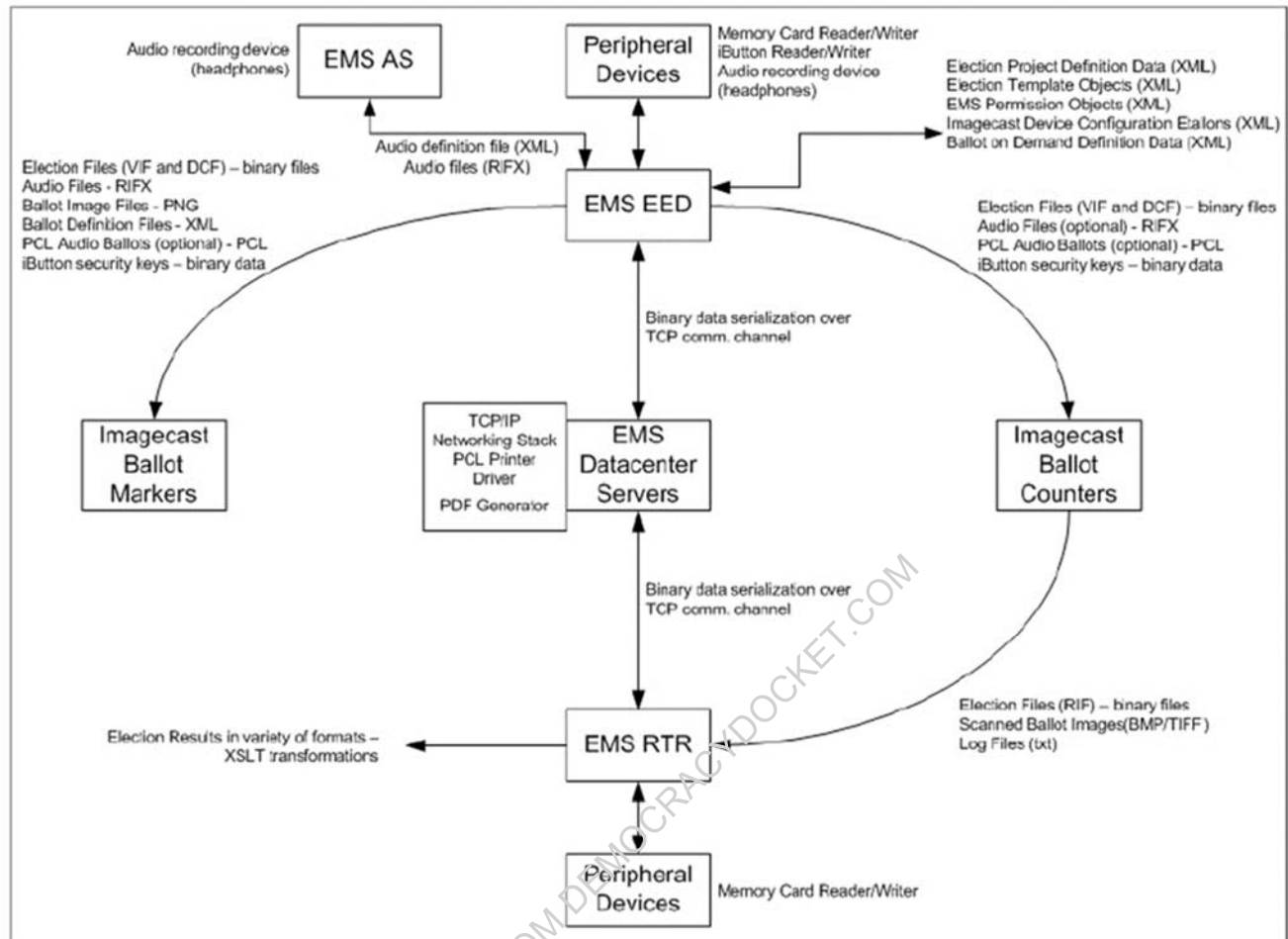
EQUIPMENT, SOFTWARE, DELIVERY DATES AND PURCHASE PRICE(S)

1. Democracy Suite (EMS) Software description

Democracy Suite is an Election Management System (EMS) that supports all ImageCast voting channels: early votes, vote by mail votes, Election Day votes from touchscreen ballot marking devices (ICX) and Scanner, and Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) votes, from a single comprehensive database.

The structure of the election files, as well as the content of the iButton security keys, is bit-level sensitive with regards to accuracy and precision. This means that a single bit change can influence system behavior. The structure of these interfacing entities is dependent on the election domain business logic implemented within the system. Therefore, within the EMS EED application, election files and iButton security keys can only be created when the election project is in the “ballot generated” state.

From an accuracy point of view, CRC checks are implemented. From a security point of view, election files utilize SHA256 (keyed hash HMAC) or digital certificates and AES encryption for data integrity and confidentiality. The figure below presents an overview of the EMS interfaces, focusing on the Democracy Suite internal and external entities.



The Democracy Suite system includes the following Third Party Software:

EMS Standard Server Prerequisites

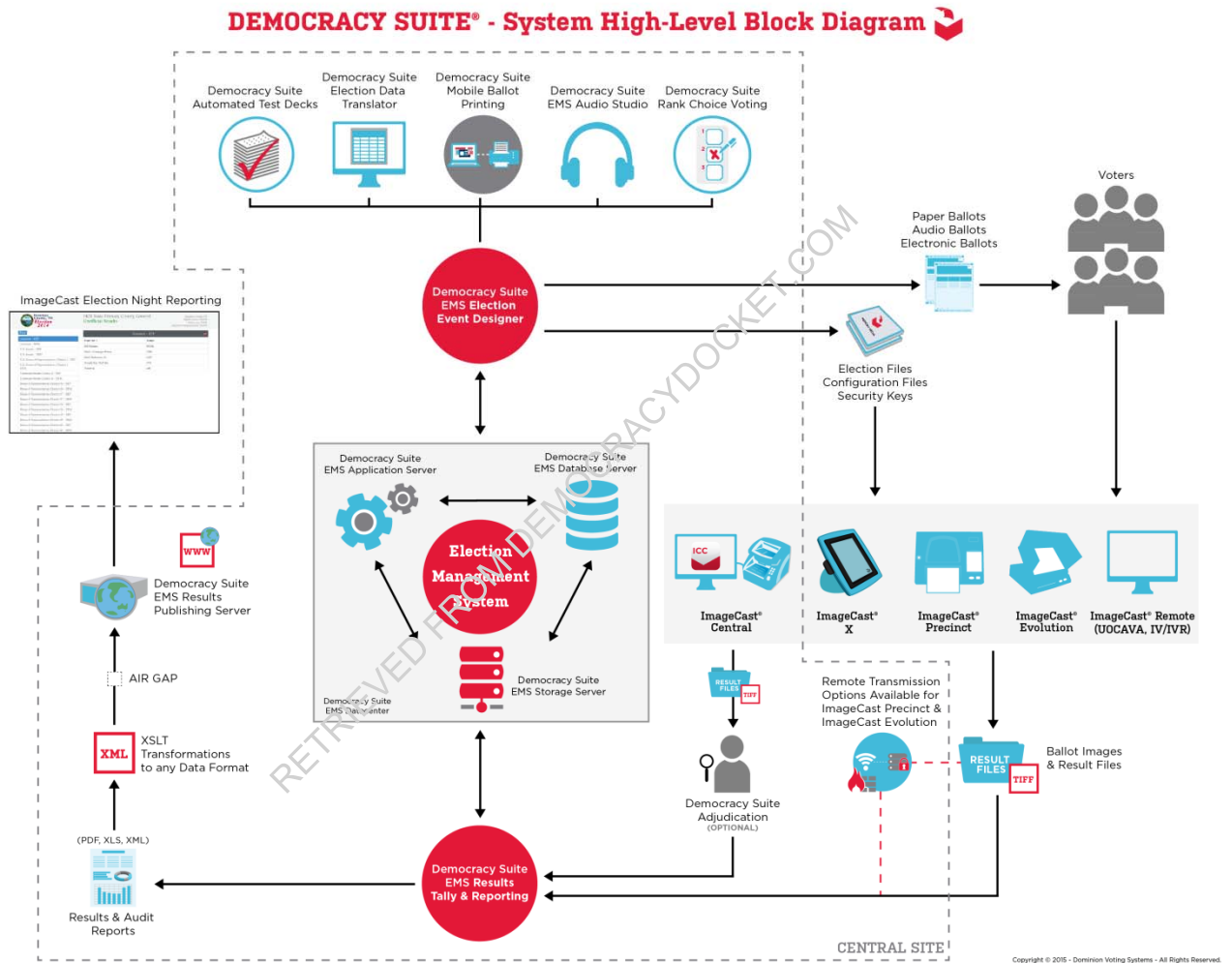
- Microsoft Visual J#
- Microsoft Visual C++ 2013 Redistributable Package
- Microsoft Visual C++ 2013 Redistributable Package (64bit)
- Microsoft Visual C++ 2015 Redistributable Package (32bit)
- Microsoft Visual C++ 2015 Redistributable Package (64bit)
- Java Runtime Environment
- Microsoft SQL Server 2016 Standard -(Microsoft SQL Server Management Tools)
- Cepstral Voices
- Arial Narrow Fonts

EMS Client Workstation Prerequisites

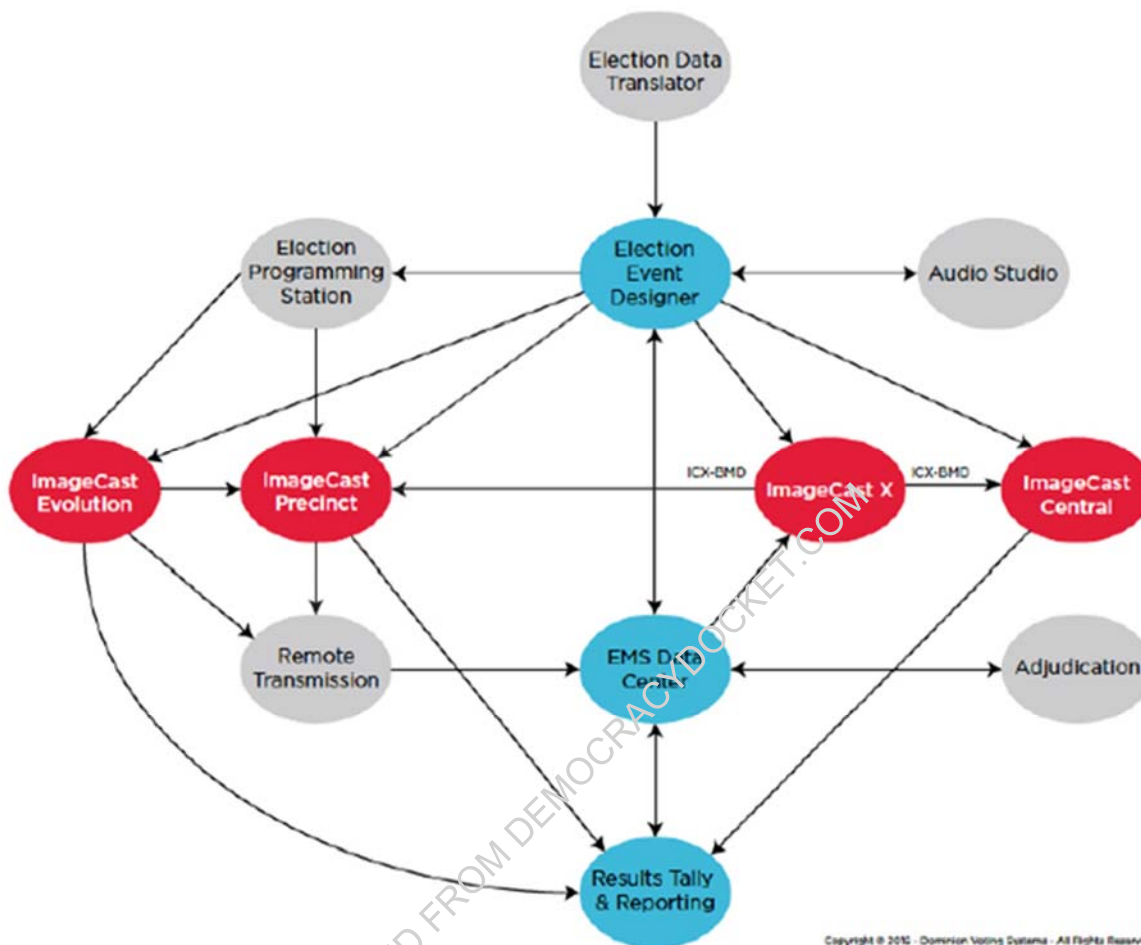
- Microsoft Visual J#
- Microsoft Visual C++ 2013 Redistributable Package
- Microsoft Visual C++ 2015 Redistributable Package 64bit
- Java Runtime Environment
- Maxim iButton Driver
- Adobe Reader
- Microsoft Access Database Engine
- Open XML SDK 2.0 for Microsoft Office
- Arial Narrow Fonts

Adjudication Workstation Prerequisites

- Dell Latitude T3420 Laptop
- Microsoft Visual J#
- Microsoft Visual C++ 2013 Redistributable Package
- Microsoft Visual C++ 2015 Redistributable Package 64bit
- Java Runtime Environment
- Adobe Reader



DEMOCRACY SUITE® - Data Flow between System Components



The Democracy Suite EMS consists of the following Dominion Software modules:

1.1 Election Event Designer (EED). EED application is used for the definition and management of election event. EED contains all ballot content utilized to define election projects. Each election project is represented as an instance of the election domain database with associated set of election project file. The definition of the election project can be initiated by importing the election data through the Election Data Translator (EDT) module from external systems that contain the necessary relational data to build a ballot or by defining election project entities without importing external data. It is important to note that an election project initiated through EDT can be further modified within the EED Client Application. The EED module can generate two types of paper ballots:

- Proofing ballots – ballots produced to allow election project stakeholders to proof ballot content and styling. These ballots cannot be processed by the ImageCast as they don't have proper ballot barcodes. These ballots are overprinted with the text "Proofing Ballots – date/time".
- Official ballots – represent production ready, press ready ballots in PDF format with barcodes and without any overprinting.

- 1.2 Results Tally and Reporting (RTR). RTR application is used for the tally, reporting and publishing of election results. For the RTR module, inputs represent encrypted and signed election result files, log files and scanned ballot images with Dominion’s patented AuditMark, produced by the ImageCast Precinct and Central tabulators (PNG and TIFF images). Outputs represent a variety of election result reports, as well as auditing information (XML, HTML, CSV, MS Excel and PDF formats).

The program uploads the result files into the results tally module, and consolidated results are verified, tabulated, and published. Once the vote data is uploaded into the result tally module, the flow of results to the public and media can be controlled.

RTR allows election officials to review the results before releasing them, and the system provides a number of reporting methods, including but not limited to summary and precinct-level (Statement of Votes Cast) result reports. In addition to the static, pre-defined reports found in most reporting systems, RTR summary and precinct-level reports use the Microsoft SQL Server reporting services engine to offer maximum flexibility to user. These reports feature a variety of configurable options and filters, including detailed breakdowns of provisional ballots cast, ballots cast during early voting, on Election Day, and by mail.

- 1.3 Adjudication. The adjudication module is used to review and adjudicate ImageCast ballot images. The application uses tabulator results files and scanned images to allow election administrators to electronically adjudicate ballots requiring review based on exception criteria. Exceptions include overvotes, undervotes, blank contests, blank ballots, write-in selections, and marginal marks. After a ballot is adjudicated, the ballot image is appended with a record of that decision including the user’s name, action taken by the user, and date and time of the action. This adjudication AuditMark is appended to the ballot image under the original AuditMark, which was manifested during tabulation.
- 1.4 Audio Studio (AS). Audio studio uses Cepstral, a third-party text-to-audio synthesizer, to automatically generate audio ballots for the ImageCast X Ballot Marking Device. The State also has the option to import human-recorded audio, with or without the use of Audio Studio. Pronunciation may be modified using the Cepstral’s Swifttalker application. The system outputs audio ballots (PNG images, SPX audio files and XML definition files), definition reports (XML, Excel or HTML files), and election definition files required to program the ImageCast X.
- 1.5 Automated Test Deck (ATD). ATD is an application used to create test decks for running Pre-Logic and Accuracy Test with marking pattern requirements. The application can be used to access the election database and produce a set of print-ready PDFs and results tables for testing.

2. EMS Hardware description, including third-party software components.¹

Description
EMS STANDARD SERVER DELL POWEREDGE R640 RACK SERVER - 16GB RAM, 6 X 1.2TB HDD, WINDOWS SERVER 2012 R2, MICROSOFT SQL SERVER 2016 STANDARD
SQL SERVER 2016 LICENSE W/5 CALs
VOICE SYNTHESIS SOFTWARE LICENSE, ALLISON - ENG - CEPSTRAL 6.2

¹ All equipment is subject to change dependent upon product availability. An equivalent model, certified by the State of Georgia, may replace products that are end of life.

Description
VOICE SYNTHESIS SOFTWARE LICENSE, ALEJANDRA SPA - CEPSTRAL 6.2
VOICE SYNTHESIS SOFTWARE LICENSE - SAVE TO FILE FOR WINDOWS
VOICE SYNTHESIS SOFTWARE LICENSE - AUDIO DISTRIBUTION LICENSE
VOICE SYNTHESIS SOFTWARE LICENSE - CONCURRENT PORT FOR WINDOWS
ANTI-VIRUS - AVAST! ENDPOINT PROTECTION SUITE, 5-PACK LICENSE
POWERCONNECT X1026 24 PORT ETHERNET SWITCH
SERVER UPS: UPS 1500VA - 2U
SERVER RACK: 12U
24" SWIVEL CAPABLE MONTIOR
VGA CABLE – MALE TO MALE, 6 FT
PATCH CABLE, CAT6, 25 FT., BLUE
EMS EXPRESS SERVER DELL PRECISION T3420/3430 WORKSTATION - 16GB RAM, 2X 500GB HDD, RAID 1, WIN 10 PRO, KB & MOUSE
8 PORT SWITCH X1008
24" SWIVEL CAPABLE MONITOR
IBUTTON PROGRAMMER KIT
COMPACT FLASH CARD READER - KINGSTON
VOICE SYNTHESIS SOFTWARE LICENSE, ALLISON - ENG - CEPSTRAL 6.2
VOICE SYNTHESIS SOFTWARE LICENSE, ALEJANDRA SPA - CEPSTRAL 6.2
VOICE SYNTHESIS SOFTWARE LICENSE - SAVE TO FILE FOR WINDOWS
VOICE SYNTHESIS SOFTWARE LICENSE - AUDIO DISTRIBUTION LICENSE
VOICE SYNTHESIS SOFTWARE LICENSE - CONCURRENT PORT FOR WINDOWS
EED/RTR/ADJ - CLIENT DELL PRECISION T3420/3430 (INTEL I5-6500, 8GB RAM, 500GB HDD, W10X64PRO) W/24" MONITOR, KB & MOUSE
SINGLE IBUTTON PROGRAMMER WITH USB ADAPTER, IBRW-100A
USB TO 1-WIRE/IBUTTON ADAPTER
PATCH CABLE, CAT6, 25 FT. , BLUE
SMART CARD READER / WRITER
COMPACT FLASH CARD READER - KINGSTON
SQL 2016 USER USER CALs

3. ImageCast X -Prime Touchscreen Ballot Marking Device (ICX-BMD)

- 3.1 Application: ImageCast X-Prime BMD is a touchscreen in-person voting device and ballot marking device. Voting sessions are initiated on the tablet by either a smart card or the entry of a numeric code based on activation. The ballot is loaded directly onto the standalone device. All voting activity is performed at the tablet, including accessible voting. Accessible voting interfaces connect to the tablet via an Audio Tactile Interface or ATI. For all modes of voting, after the voter reviews the ballot selections, a paper ballot is created for the voter from a printer in the voting booth. The printed ballot contains a written summary of the voter's choices, as well as a 2D barcode which is read by Dominion's ImageCast Precinct or Central tabulator. No votes are stored on the ImageCast X-BMD unit. All votes can be tabulated and stored both the ImageCast Central and Precinct Tabulators.
- 3.2 Components: ImageCast X-Prime BMD is composed of a 21.5" Avalue touchscreen, Android OS 5.1, DC 19V input, HP LaserJet Pro M402dne laser printer.
- 3.3 Additional included items: Three (3) ICX smartcards (to be used for activation, pollworker or technician), battery, 6' cable and 8GB flash drive.

4. ImageCast Precinct Tabulator (ICP)

ImageCast Precinct Scanner and Tabulator is an optical scan ballot tabulator used to scan marked paper ballots, interpret voter marks on the paper ballot, communicate these interpretations back to the voter and upon voter acceptance, deposits the ballot in the ballot box. The ImageCast consists of the following:

- 4.1. Two (2) optical imaging scanners for creating a duplex scanned image of each side of the ballot. Ballots can be fed in all four (4) orientations.
- 4.2. Linux Operating System.
- 4.3. Two memory cards ports for storage capabilities. Two (2) 8GB memory cards are provided and located behind two securable doors (Administrator Door and Pollworker Door).
- 4.4. An integrated interactive electronic display in the form of an ultra-high contrast graphical color 5.7" LCD screen, and a built-in touch screen for administration purposes.
- 4.5. An internal 3" thermal printer and one (1) 3" paper roll for generating reports.
- 4.6. Two (2) administrative security key (iButton) used with an integrated receptacle (physically attached to the top of the unit and electrically connected to the motherboard) used for a variety of verification and security tasks such control, data confidentiality and integrity functions.
- 4.7. A motorized paper feed mechanism for detecting and moving the ballot within the scanner. Ballots used with the ImageCast must be 8.5" wide by a variable length (11", 14", 17" and 22"). The paper feed mechanism is physically capable of moving the ballot forward into the machine, across image sensors, enabling complete image capture of both sides of the ballot.
- 4.8. Power supply module uses 120 Vac, 60 Hz, one phase power. It has a power consumption of 0.07 Amps at 120 Volts AC.
- 4.9. An internal battery which is rated to provide two-and-a-half (2.5) hours of normal use in the absence of AC power. In addition to internal 2.5 hours battery an internal 6 hours battery option is also available. There is also a connection for an external 12VDC SLA battery.

- 4.10. Patented functionality known as the AuditMark. For each ballot scanned and accepted into the unit, a corresponding ballot image is created and stored for audit purposes. The image consists of two parts described below.
- The top portion of the image contains a scanned image of the ballot.
 - The bottom portion consists of a machine-generated text showing each mark that the unit interpreted for that particular ballot. This is referred to as the AuditMark.

5. **ImageCast Central Scanner (ICC)**

The ImageCast Central Scanner consists of a commercial off-the-shelf digital scanners configured to work with the ImageCast Central Software for high speed ballot tabulation. Each ImageCast Central Scanner includes the following components:

- 5.1. Canon DR-G1130 high speed document scanner
- 5.2. ImageCast Central Software including third party Twain software
- 5.3. DELL 7450 Computer 24" Touchscreen DELL Optiplex AIO 3050 Touchscreen
- 5.4. iButton Security Key
- 5.5. iButton Programmer and iButton Key Switch & Cat5 R.J 45 Cables used with Democracy Suite to transfer security and election information to the iButtons for use with the ICC.
- 5.6. Patented functionality known as the AuditMark. For each ballot scanned and accepted into the unit, a corresponding ballot image is created and stored for audit purposes. The image consists of two parts described below.
 - The top portion of the image contains a scanned image of the ballot.
 - The bottom portion consists of a machine-generated text showing each mark that the unit interpreted for that particular ballot, known as the AuditMark.

6. **ImageCast Molded Plastic Ballot Box**

A textured molded plastic ballot box per ImageCast Precinct unit. The ballot box is made of a three (3) compartments, custom designed for use with the ImageCast Precinct.

7. **Voting Supply Carriers.** Design and manufacture mobile Voting Supply Carrier that will store, secure and transport voting equipment and will act as a mobile vote center.

8. **System Security Description**

Dominion implements security protocols that meet or exceed EAC VVSG 2005 requirements. All of Dominion's security protocols are designed and implemented to stay current with the rapidly evolving EAC security requirements set forth by various iterations of the VVSG. Dominion's security technology is unprecedented insofar as it takes into account every aspect and every component of the Democracy Suite platform. This includes – but is not limited to – the full encryption of election projects, iButton security keys, memory cards, election data, software applications, and elections results files. In addition, Dominion developed a custom ballot authentication system built around an secure ballot paper stock and in-tabulator authenticators.

Democracy Suite integrates a role-based access control system for all software and hardware components. Each user accessing the system is the member of one of the predefined or custom-made roles. Each role has its own set of permissions, or actions that users of that role are allowed to perform. This access control approach provides authentication and authorization services and can be granular according to the jurisdiction's needs and organization. Complete

user and role membership management is integrated within the Democracy Suite EMS Election Event Designer client module.

The Democracy Suite EMS platform implements role-based user management for provisioning access control mechanisms on each election project. Managing access control policies is integrated within the User Management activity of the EMS EED module. This activity is permitted only for users with administrative privileges.

Democracy Suite utilizes hardware-based security tokens (iButton security keys) in the process of access control for ImageCast Precinct tabulators. These password paired hardware tokens contain data encryption information used in the voting process (encryption and signing keys). Without a valid security token, and paired access password, the administrative functions of election tabulators are effectively locked.

All of these activities and controls, and more described below in response to specific section requirements, are integrated within the Democracy Suite platform. 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.

8.1 Password configurations

Proper password management relies on multiple activities and controls, namely:

- Input data validation
- Data quality
- Utilization of one-way (hash) cryptography
- Computer generated passwords for greater entropy and protection from dictionary attacks
- Different password strength profiles for different user levels
- Utilization of hardware tokens for storing user credentials (two-level authentication security: something you know and something you have)
- User state machine (initial, active, inactive)

The system does not enforce aging or complexity, but Dominion recommends establishing best practices that meet State's requirements.

8.2 Authentication configuration

To protect any modification of software by malicious users, the Democracy Suite Election Management System integrates the Microsoft .NET Framework code signing process, within which, Dominion digitally signs every executable and library (DLL) during the software build procedure. After the installation of Election Management software, only successfully verified EMS software components will be available for use. Digital signature verification is performed by the .NET Framework runtime binaries. If a malicious user tries to replace or modify any EMS executables or library files, the digital signature verification will fail and the user will not be able to start the EMS application.

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. The Democracy Suite Election Management System uses these techniques to encrypt election files prior to their use on ImageCast tabulators. Once the polls have been closed, the ImageCast tabulators encrypt all of the results files prior to transmitting them back to EMS.

SHA-256 hashes are used for all data integrity and verification. Should an intrusive process or altering of any file occur, hash values will be, in turn, altered as well. Any presence of an intrusive process will be detected, as the hashes of any altered data will not match the value initially determined.

For communication channels (as well as data storage) a combination of security techniques for data integrity, authenticity and confidentiality is implemented. Democracy Suite integrates AES or RSA encryption algorithms for data confidentiality, along with SHA-256 and HMAC digital signatures for data signing (data authenticity and integrity).

		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

8.4 Logging/Auditing capabilities

From the initial state of the election project, until the deactivation state, the EMS system maintains an activity log within the EMS Database. This activity log contains every action that any of the users have performed within the system and represents a detailed audit log that can be analyzed and printed in the form of an audit report. The audit record information cannot be modified or permanently deleted using the EMS client applications. It can, however, be exported for archiving purposes as part of the record retention policy. During the voting, ImageCast devices keep an activity audit log which tracks events happening on the device itself. Logs are exportable in text format.

8.9 Secure Development Process

All software programs satisfy recommended coding standards, as well as code styling guidelines as required by EAC VVSG standards. Automated code review processes are in place, that verifies compliance with industry accepted coding standards for programming languages used. In addition, proper system and software hardening procedures are clearly defined and regularly tested. Data integrity and confidentiality is also implemented according to NIST defined and FIPS validate procedures and algorithms.

9. **KNOWiNK Electronic Pollbook**

The KNOWiNK Poll Pad solution provides a seamless electronic voter check-in and verification process for election authorities across North America. Poll Pad is a secure Apple iPad application requiring no appendages for operation.

- Process voters in approximately 30 to 45 seconds; mitigate long lines with fast and secure voter look-up.
- Built-in election management and reporting tools; elections can be finalized and submitted within hours of election close.
- Customizable workflow presents required steps according to each jurisdiction's requirements and preferences.
- Improved accuracy and reduced preparation time and storage requirements with the elimination of paper logs.
- Poll workers or voters cannot leave the application without a password, preventing user error, a line slow-down, or creating a potential security issue.

The Poll Pad components include the following:

- iPad tablet - The iPad has a touchscreen/keyboard and a shockproof clear case. The iPad has a battery life of approx. 10 hours. Make: Apple | Model: MP2FLL/A
- Encoder/iOS Reader - The Mfi certified lightning port contact card reader connects securely to the iPad lightning port and include a micro USB cable. Make: FEITAN Technologies | Model: iR301
- iSync Drive - KNOWiNK's secure proprietary removable memory device, the iSync flash drives. Make: KNOWiNK | Model: iSD-110
- Stand for iPad - The iPad stand is durable and user friendly. Make: AI Data | Model: i360
- Scanning tray - KNOWiNK'S patented scanning trade scans barcodes on voter ID cards or state identification cards. Make: KNOWiNK | Model: ISP103b-KN2-1
- Styluses - Poll workers and voters may use the styluses or their finger for the iPad's capacitive touch screen. Make: AI Daata | Model: ISP-1010-KNO
- Carrying case - Shockproof weatherproof foam-fitted case. Make: Nanuk | Model: 910

10. **Implementation Services**

10.1 **Implementation Phase Periods**

The implementation period will consist of a sixteen-month implementation; Phase One includes a pilot of 6 counties and the GA Secretary of State office for the November 2019 General elections. Phase Two includes the 2020 Presidential Preference Primary and all Primary, General, Runoff and Special elections for all 159 counties in Georgia as well as the state in the 2020 Election cycle.

10.2 Implementation Plan and Schedule

Dominion's Project Manager and the State's Project Manager shall provide an Implementation Plan specifying the details for all tasks necessary to successfully complete the project, working cooperatively to set hard and soft deadlines. Each task identified will include a start and end date and the responsible parties involved. The Implementation Plan will include, but will not be limited to, a detailed Implementation Project Plan, which includes product delivery with implementation, delivery and training dates; Acceptance Testing Plan; System Readiness Plan; a Training Plan specifying training dates and curriculum to parties requiring training; as well as a Communication Plan. Please see a draft Project Plan attached hereto.

The draft Project Plan developed for this Agreement represents the sample based upon discussions with the State. Upon execution of the Agreement, the Parties shall finalize the project plan including the training and delivery schedule. The Parties agree that during the course of the implementation, changes to the project schedule may be required. Any changes to the project schedule must be mutually agreed to by both Parties and such agreement shall not be unreasonably withheld.

10.3 Project Team

Dominion's project team includes key experienced staff, with extensive expertise in system implementation, project management and customer service obtained through years of dedicated work for our customers. The personnel selected for the State of Georgia's implementation are among Dominion's most experienced team members, ensuring that Georgia has the best people to meet their needs and requirements. The team will receive executive oversight from the Executive Vice President of Sales and Executive Vice President of Operations throughout the project.

Project Manager. The Dominion Project Manager will be appointed and dedicated entirely to this project and will be on-site, full-time (consistent to the departments work hours) and available commencing shortly after the contract is signed through completion of the first year. Dominion's Project Manager will be responsible for arranging all meetings, visits and consultations between the Parties and for all administrative matters such as invoicing, payments and amendments. The Dominion Project Manager shall have the requisite skills and experience to provide the services required for the implementation including without limitation: elections support, project management, excellent verbal and written communications skills, strong organizational skills to include multi-tasking and time management skills, and ability to manage detail-oriented projects with fixed deadlines. Dominion shall make commercially reasonable efforts to provide a Project Manager familiar with the election operations, and the election rules and regulations of Georgia.

The Dominion Project Manager shall communicate with the State as to the status of information, milestones, procedures and progress on the tasks as set out in this Agreement and to advise the State forthwith upon the occurrence of any event requiring a material change in such plans, and request Customer's written consent to any such material change. In addition, the following Project management resources will be dedicated on an as need basis through the 2020 general election.

After the 2020 general election, Project Management will continue through the remainder of the Agreement. After the completion of the implementation, a Customer Relations Manager will work directly with the State (both on and off site), but will have other responsibilities outside of the Agreement. In addition, account management and technical phone support shall be available through the contract Term at no additional costs.

Product Specialist. Dominion Voting shall provide technical support throughout the implementation. This resource is responsible for the installation, operation, repair, and maintenance of all Dominion Voting Systems hardware and software, scheduling and supervising resources for all hardware and software related matters. The Product Specialist will provide election support services and customer training, and interfacing directly with customers, co-workers and election officials.

System Technical Manager. Shall work with the State's elections staff, as well the State's IT staff, to install the certified EMS and adjudication system hardware. As part of this role, the systems configuration manager will evaluate the current environment at the County and provide recommendations for any changes required for configuration.

Training and Documentation Manager. Will coordinate with Dominion and County project managers to develop and customize all training documentation and supervise all training related activity.

Election Programmers. Responsible for all aspects of election event definition, including without limitation to following components: Importing of data files into the EMS system, defining election project parameters and assigning templates, assigning tabulators (ICC, tablet, mobile ballot printing), defining ballot structures, creating proofing ballot, creating official ballots, and creating election files and the security keys for the ImageCast®.

Ballot Printer Certification Manager. Shall conduct activities required to qualify the County certified printer as described in [section six] of this Agreement.

Other. Additional Acceptance and Readiness Testing, Pre-Logic and Accuracy, Election Day rover personnel, and Post-Election activity (recount and canvass).

10.4 System Transition Review

This meeting is a key meeting with the objective of: reviewing the project plan; confirming major milestones, key dates and deliverables; and developing the Implementation Plan.

Discussion items will include: Confirming ImageCast quantities, ImageCast delivery plan and schedule, consumables, election programming, ballot definition and required resources. Demonstration of the ImageCast units, training, testing, simulation services and managed election services are also discussed for a successful delivery.

Gap Analysis - After an initial gap analysis, a simulation event further uncovers implementation, deployment, usability, and customization requirements. All of these details are funneled into Dominion's implementation process, which includes (as realistically as possible) the customer in scheduled development iterations.

In order to ensure that the system meets the State of Georgia's business and technical requirements, Dominion will work closely with State elections staff to identify, prioritize and enable the roll-out of these requirements through each phase of the implementation.

At the end of each stage, a report will be created to summarize the shared understanding of the requirements, and the State will have a chance to provide feedback and formal sign-off as acceptance.

10.5 System Installation and Configuration

Dominion's Project Manager will manage the shipment process through an authorized shipper to ensure delivery is successful. The State's staff is also responsible for the removal of all legacy equipment. Dominion's Project Manager will require a written confirmation ensuring that all packages were delivered successfully.

10.6 Acceptance Testing

Dominion shall provide an Acceptance Test Plan (ATP). The ATP shall identify all tests necessary to demonstrate compliance with the requirements of the State of Georgia. Dominion shall be responsible for

providing all training and training materials required to support the acceptance testing. Dominion and the State shall finalize the development of the test plan and procedures prior to the acceptance-testing phase.

A Dominion hardware technician will provide guidelines to the team responsible for the State warehouse for inbound acceptance testing. This includes assessing suitability and identifying any modifications required, identifying areas for each process including a secure area for inventory control, preparing necessary acceptance documentation, and ensuring all necessary supplies are available for work.

A checklist template will be provided to the State for printing and distribution during the acceptance test process. For each piece of ballot marking equipment, State staff, under the supervision of a Dominion technician, will complete the acceptance test for each unit received. Each form will be signed and stored by the State with copies made or scanned for Dominion in order to ensure that each component is in proper working order upon receipt and unpacking.

10.7 Printer Certification

Ballot qualification is an educational and testing process designed to assist ballot printers on how to properly print ImageCast ballots and maintain an ongoing level of quality assurance needed to ensure the ballots they provide their customers will tabulate correctly. ImageCast printing qualification is also meant to be an ongoing support vehicle providing qualified printers with an ongoing resource to continually assist printers if questions were to arise. The printer certification process consists of 5 stages: Administrative; Discovery; Training; Testing; and Qualification.

10.8 Election Setup

Election Definition

Dominion's Democracy Suite Election Management System shall have the capability of importing election data from the State of Georgia's current database to generate ballot layout used to conduct an election. Dominion shall provide election definition services for the 2019 pilot and 2020 elections. In the event the State requests additional election definition services from Dominion, Dominion shall provide those services according to the prices identified in the pricing Schedule.

The State shall review and approve or identify issues to all Dominion deliverables related, with particular attention to ballot proofs and audio files, to such service within two (2) business days of discovery of an issue by the State. In the event the State discovers an issue, it shall provide written notice to Dominion following the discovery of any issue and Dominion shall rectify the issue at no additional cost to the State. In the event the State approves the final ballot proofs and audio files and subsequent to such approval, requests that a change be made to the deliverable, the Dominion may provide the change according to the service pricing identified in pricing schedule.

Ballot Layout

Dominion's Ballot Layout/Generation System supports both English and Spanish both in written and audio format; and, have the ability to add new languages. Dominion's System has the ability to import data in all languages via direct importation to appropriate files or cut and paste. The State will be able to edit all ballot layout files in all languages.

Dominion's System creates all ballots, (precinct, vote center, absentee, and audio) from a single Election Management System. Dominion's Ballot Layout/Generation System has audio capability utilizing human voice recordings as well as voice simulation program.

Dominion's Democracy Suite election management system can support a single input of customer profile data such as voting locations, precincts, political subdivisions, offices, parties and machines; and use this data to simultaneously manage multiple elections by multiple users.

Dominion shall work with the State and the certified printer used by the State and Counties to create a simple method of transferring ballot information to the printer for production.

Dominion will work with the State to develop the appropriate workflow to import the candidate/contest information directly from the State of Georgia's current Election Information Management System and create the absentee ballot, BMD ballot, and sample ballot from the same imported file.

Logic and Accuracy Test

On completion of election definition and ballot layout, the ballots are generated. Ballot proofs and electronic ballot image files are generated and provided to the State. The State and Counties carefully reviews each ballot. When the State is satisfied that the ballots are correct, they initial each ballot, and when they are satisfied that all ballots, audio and reports are correct, they sign-off on their accuracy, and the image files are provided to the printer.

Ballot printing and distribution are the responsibility of the certified printer and the State/Counties. Dominion will provide a recommended ballot inspection process that should be followed to ensure that all ballots produced are of sufficient quality. The receipt of test ballots from the certified ballot printer is the milestone that triggers the beginning of Pre-Election Logic and Accuracy Testing ("Pre-LAT"), a simulation of the voting process under which the System will operate.

Election files are transferred from the EMS to memory cards which are created for each ICX ballot marking device, ICP tabulator and the ICC system. The State is responsible for delivering the election files to the Counties. The State, Counties, or Dominion will then load the election files onto the units. After loading the election files onto the units, Pre-LAT must be performed on all System components before deployment.

With a paper-based tabulation system, Pre-LAT is performed on the ImageCast X, ImageCast Precinct and ImageCast Central tabulators through the use of ballot test decks, rather than simulation scripts. Generally, the Pre-LAT procedure involves programming all voting machines with the final election definition and scanning hand-marked or pre-marked (computer generated) test decks through each tabulator. This provides verification of both the quality of the printed ballots as well as the correctness of each tabulator's programming. After test decks have been scanned and the results report tapes have been verified, test results may be uploaded directly to the EMS Server using EMS Results Tally and Reporting. This result transfer test verifies that all parameters for each tabulator have been correctly configured.

10.9 Election Support

The Dominion project team will develop a customized support plan to meet the needs of the GASOS and counties for the November 2019 Pilot elections through the 2020 election cycle. This plan will include technical support for GASOS and counties on election night including the day before to the day after the election. This support plan defines the number of Dominion staff required in the field on election day as well. Dominion's on-site support resources have the necessary skills to assist the State to ensure the polling location opens in a timely fashion and that the equipment functions properly. In addition, a key role for the on-site support resource is to assist the State and counties with polling place closing, tabulation and results reporting. Dominion's active voting support strategy will be customized to meet the State's and counties specific needs.

10.10 Post-Election

Canvass - Dominion will assist the State/Counties in creating procedures for the conduct of the canvass and any necessary recounts. The system shall provide canvass reports including, but not limited to Interim, Semi-Final Official, Final Official, and the Statement of Vote reports. Dominion will be available to assist the State's or County's staff in the conduct of the canvass and for any recounts through the 2019 – 2020 Election Cycle. Dominion shall provide sample procedures and recommendations for the canvass process.

Recount - The system must be able to provide for a manual recount process that would utilize either the physical ballot or ballot image with AuditMark, Cast Vote Record and EMS SOV reports. Dominion will assist the State/County in creating procedures for a recount.

ATTACHMENT 1 TO SOLUTION ORDER

Installation Site Specifications

ICX

For best lifetime, follow the storage recommendations described below for the ImageCast X:

- Operating Temperature min/max: 0°C~40°C
- Storage Temperature min/max: -20°C~60°C
- Operating and/Storage Conditions (Relative Humidity): From 0%~90% RH non-condensing
- Pack the ImageCast X tablet into its provided packaging box with foam inserts to provide vibration and impact protection.

The ImageCast X units should not be stacked on top of one another for storage unless they are in their respective carrying cases or packaging boxes (Maximum Stack = 5 Boxes High).

Standard power / electrical outlets.

ICC

For optimal product of the ImageCast Central, storage limitations should adhere to the following specifications:

- Storage Temperature min/max: -40°C~65°C
- Operating and/Storage Conditions (Relative Humidity): From 20%~80% (non-condensing)
- Place the CPU and Scanner in packaging boxes with foam inserts to provide vibration and impact protection
- Store the packaged CPU and Scanner boxes under conditions specified
- Store the CPU and Scanner boxes in a dust-free, clean environment
- The CPU and scanner units should not be stacked on top of one another for storage unless they are in their respective carrying cases or packaging boxes (Suggested Maximum Stack = 5 boxes high for CPU and 4 boxes high for the G1130 scanner)

Standard power / electrical outlets.

ICP

For optimal ImageCast Precinct product life, storage limitations should adhere to the following specifications:

- Storage Temperature min/max: From -25°C - 60°C
- Operating and/Storage Conditions (Relative Humidity): From 20% - 80% RH non-condensing
- Place the tabulator inside the re-sealable bag into the provided packaging box with foam inserts to provide vibration and impact protection.
- Store the packaged tabulator box under conditions specified.
- Alternatively, leave the tabulator on the ballot box but place the ballot box dust cover over it to keep it free from environmental elements.
- Store the tabulator (and ballot box, if applicable) in a dust-free, clean environment.
- Perform periodic charging of the back-up battery module for 12 hours every 9 months.

- The tabulators should not be stacked on top of one another for storage unless they are in their respective carrying cases or packaging boxes (Suggested Maximum Stack = 4 Boxes High).

Standard power / electrical outlets.

Server Dell PowerEdge R630

Temperature Specifications

Storage -40°C to 65°C (-40°F to 149°F)

Continuous operation (for altitude less than 950 m or 3117 ft) 10°C to 35°C (50°F to 95°F) with no direct sunlight on the equipment.

NOTE: Maximum of 145 W 22 core processor is supported in systems with eight 2.5-inches drives, two PCI slot chassis, and 75 W single wide active GPU.

Maximum temperature gradient (operating and storage) 20°C/h (36°F/h)

Standard power / electrical outlets.

RETRIEVED FROM DEMOCRACYDOCKET.COM

ATTACHMENT 2 TO SOLUTION ORDER

Functional Requirements

	System Capacity	
1	System accommodates for a minimum of three (3) different languages	Comply
	Ballot Secrecy	
2	System must not allow ballot to be traced to voter	Comply
	Special ballot voting circumstances	
3	System must allow for write-in candidate for all offices with post-election review of write-in votes readily available	Comply
4	System must prevent voter from casting an overvote (voting for more candidates than allowed for an office)	Comply
5	System must notify/alert voter if they failed to vote for one or more offices or propositions	Comply
6	System must allow a voter to change a vote during the process prior to casting	Comply
7	System must have secure mechanisms for insuring that all ballots cast are authorized by the pollworkers in that precinct	Comply
	Ballot Types	
8	Accommodate for no fewer than six (6) political parties in a primary election	Comply
9	System must accommodate for hundreds of ballot styles to account for split precincts which may have several unique voting districts	Comply
10	System must allow all voters to be capable of casting a ballot independently, without assistance or without the intervention of pollworkers, in all elections	Comply
11	System capabilities for mobility-restricted voters	Comply
12	System capabilities for visually-impaired voters with audio component	Comply
13	System capabilities for voters with limited or no manual dexterity	Comply
14	System must accommodate last-minute ballot changes due to court orders quickly and effectively	Comply
15	System must be capable of performing self-test to identify equipment errors	Comply
16	System must be able to produce a paper “zero tape” evidencing the fact that the System has no votes recorded on it at the opening of the polls	Comply
	Results tabulation	
17	System must produce a paper record once the voter has finished voting of each voter's choices	Comply

18	System must have the capacity to maintain internal back-ups of the votes that have been cast on the System	Comply
19	System must include a software component that produces a final, unified tabulation of the votes cast in the precincts, and any centrally cast or tallied ballots (such as votes-by-mail and early votes), including provisional votes	Comply
	Storage	
20	System includes all necessary equipment to optimally store its components	Comply
21	System requires only standard electrical outlets to keep components charged and use-ready	Comply
22	System components do not require temperature or humidity conditions outside of industry standard storage facilities	Comply
	Maintenance	
23	After the period of vendor-supplied maintenance expires, the system is capable of being maintained by the County staff.	Comply
24	Vendor guarantees the availability of replacement parts for a period of 10 years after system acquisition.	Comply
	Touchscreen Display	
25	Touchscreen component includes variable screen fonts	Comply
26	Touchscreen allows voter to vary screen font size	Comply
27	Touchscreen allows contrast of screens to be varied	Comply
28	Touchscreen Allows voter to vary screen contrast	Comply
29	Touchscreen component includes variable screen contrast	Comply
30	Touchscreen component allows voter to freely move from screen to screen	Comply
31	Touchscreen component includes review function after voter has viewed all ballot pages	Comply
32	Touchscreen component allows voter to go directly from review page to page where a change in vote can be made	Comply
33	Touchscreen component prevents offices from being split onto multiple screens	Comply
34	Touchscreen component prevents overvoting for an office or proposition	Comply
35	Touchscreen component includes messages relating to successfully ballot casting	Comply
	Ballot Printer	
36	Printer is easily refilled with paper	Comply
37	Printer uses industry standard connectors and ports	Comply
38	System can produce a flat file of the summary report to be posted on the web sites of the State	Comply

ATTACHMENT 3 TO SOLUTION ORDER

RESERVED

RETRIEVED FROM DEMOCRACYDOCKET.COM

ATTACHMENT 4 TO SOLUTION ORDER

Implementation Schedule including standard Milestones

Task Name	Duration	Start	Finish
GA Draft Project Plan			
Installation Key Dates	123 days	Thu 8/1/19	Mon 1/20/20
Phase 1 Installations	69 days	Thu 8/1/19	Tue 11/5/19
Phase 2 Part 1 Installations	40 days	Wed 11/6/19	Tue 12/31/19
Phase 2 part 2 Installations	14 days	Wed 1/1/20	Mon 1/20/20
Election Key Dates	261 days	Tue 11/5/19	Tue 11/3/20
2019 General Election	1 day	Tue 11/5/19	Tue 11/5/19
PPP	1 day	Tue 3/24/20	Tue 3/24/20
Primary Election	1 day	Tue 5/26/20	Tue 5/26/20
Primary Election Runoff	1 day	Tue 7/28/20	Tue 7/28/20
General Election	1 day	Tue 11/3/20	Tue 11/3/20
Project Management	383 days	Tue 7/16/19	Thu 12/31/20
Project Initiation	14 days	Tue 7/16/19	Fri 8/2/19
Review Project Structure, roles and responsibilities	11 days	Tue 7/16/19	Tue 7/30/19
Review and update project plan	11 days	Tue 7/16/19	Tue 7/30/19
Manufacturing and Deliveries Schedule	11 days	Tue 7/16/19	Tue 7/30/19
Issues Tracking and Escalation Plan	11 days	Tue 7/16/19	Tue 7/30/19
Risk Mitigation Plan	11 days	Tue 7/16/19	Tue 7/30/19
Communication Plan	11 days	Tue 7/16/19	Tue 7/30/19
Conflict Resolution Plan	11 days	Tue 7/16/19	Tue 7/30/19
Training Plan Finalization	11 days	Tue 7/16/19	Tue 7/30/19
Review and Adjust Training Schedules	11 days	Tue 7/16/19	Tue 7/30/19
Requirements Gathering, Gap Analysis and Application Configuration	11 days	Tue 7/16/19	Tue 7/30/19
Requirements Review	11 days	Tue 7/16/19	Tue 7/30/19
Requirements Signoff	1 day	Tue 7/30/19	Tue 7/30/19
Create Election Data Import Bridge	12 days	Tue 7/16/19	Wed 7/31/19
Customer kick-off meeting	1 day	Thu 8/1/19	Thu 8/1/19
Poll Pad Build, Testing and Documentation	54 days	Tue 7/16/19	Fri 9/27/19
Receipt and Acceptance Testing in DVS facility	25 days	Tue 7/16/19	Mon 8/19/19
Development	25 days	Tue 7/16/19	Mon 8/19/19
Migrate App Changes	1 day	Fri 8/9/19	Fri 8/9/19
Test	14 days	Mon 8/12/19	Thu 8/29/19
Create test cases	5 days	Mon 8/12/19	Fri 8/16/19
Acceptance Testing	5 days	Thu 8/22/19	Wed 8/28/19
Testing Signoff	1 day	Thu 8/29/19	Thu 8/29/19
Documentation	5 days	Mon 9/23/19	Fri 9/27/19
Create administrator and user guides	5 days	Mon 9/23/19	Fri 9/27/19
Project Meetings	371 days	Thu 8/1/19	Thu 12/31/20
Weekly Project Status Meetings	371 days	Thu 8/1/19	Thu 12/31/20

Receipt and Acceptance Testing in DVS facility	125 days	Mon 7/29/19	Fri 1/17/20
July Shipment	20 days	Mon 7/29/19	Fri 8/23/19
Receive Shipment	3 days	Mon 7/29/19	Wed 7/31/19
Initial Acceptance Test	18 days	Tue 7/30/19	Thu 8/22/19
Preparation and Delivery of Equipment	17 days	Thu 8/1/19	Fri 8/23/19
August Shipment	21 days	Mon 8/26/19	Mon 9/23/19
Receive Shipment	5 days	Mon 8/26/19	Fri 8/30/19
Initial Acceptance Test	22 days	Thu 8/22/19	Fri 9/20/19
Preparation and Delivery of Equipment	10 days	Tue 9/10/19	Mon 9/23/19
Ship 334 Poll Pads	15 days	Tue 9/3/19	Mon 9/23/19
September Shipment	23 days	Tue 9/24/19	Thu 10/24/19
Receive Shipment	5 days	Tue 9/24/19	Mon 9/30/19
Initial Acceptance Test	23 days	Mon 9/23/19	Wed 10/23/19
Preparation and Delivery of Equipment	10 days	Thu 10/10/19	Wed 10/23/19
Ship 369 Poll Pads	14 days	Mon 10/7/19	Thu 10/24/19
October Shipment	25 days	Fri 10/25/19	Thu 11/28/19
Receive Shipment	5 days	Fri 10/25/19	Thu 10/31/19
Initial Acceptance Test	24 days	Mon 10/28/19	Thu 11/28/19
Preparation and Delivery of Equipment	10 days	Fri 11/15/19	Thu 11/28/19
November Shipment	19 days	Mon 11/25/19	Thu 12/19/19
Receive Shipment	5 days	Mon 11/25/19	Fri 11/29/19
Initial Acceptance Test	13 days	Tue 11/26/19	Thu 12/19/19
Preparation and Delivery of Equipment	10 days	Fri 12/6/19	Thu 12/19/19
Ship 7047 Poll Pads	75 days	Mon 11/18/19	Fri 2/28/20
December Shipment - Any additional balance needed	25 days	Mon 12/16/19	Fri 1/17/20
Receive Shipment	5 days	Mon 12/16/19	Fri 12/20/19
Initial Acceptance Test	24 days	Mon 12/16/19	Thu 1/16/20
Preparation and Delivery of Equipment	10 days	Mon 1/6/20	Fri 1/17/20
Phase 1 Installations	69 days	Thu 8/1/19	Tue 11/5/19
November 2019 Election Day	1 day	Tue 11/5/19	Tue 11/5/19
Counties receiving equipment during Phase 1	32 days	Thu 8/1/19	Fri 9/13/19
GASOS			
County 1			
County 2			
County 3			
County 4			
County 5			
County 6			
Procurement and Delivery	32 days	Thu 8/1/19	Fri 9/13/19
Election Management System	32 days	Thu 8/1/19	Fri 9/13/19
Documentation Delivery	1 day	Thu 8/1/19	Thu 8/1/19
Installation guides	1 day	Thu 8/1/19	Thu 8/1/19
User guides	1 day	Thu 8/1/19	Thu 8/1/19
Equipment	30 days	Mon 8/5/19	Fri 9/13/19
Procurement and Delivery	30 days	Mon 8/5/19	Fri 9/13/19
Installation	30 days	Mon 8/5/19	Fri 9/13/19
County Level Acceptance Testing and Training	30 days	Mon 8/5/19	Fri 9/13/19

Tabulator and Accessible Voting System	30 days	Mon 8/5/19	Fri 9/13/19
Documentation Delivery	1 day	Thu 8/1/19	Thu 8/1/19
User Manuals	0.25 days	Thu 8/1/19	Thu 8/1/19
Quick reference guides	0.25 days	Thu 8/1/19	Thu 8/1/19
Maintenance manuals	0.25 days	Thu 8/1/19	Thu 8/1/19
Training manuals	0.25 days	Thu 8/1/19	Thu 8/1/19
Supplies and Consumables	30 days	Mon 8/5/19	Fri 9/13/19
Procurement and Delivery	30 days	Mon 8/5/19	Fri 9/13/19
County Level Acceptance Testing and Training	30 days	Mon 8/5/19	Fri 9/13/19
Training			
GASOS Training	22 days	Thu 8/1/19	Fri 8/30/19
D-Suite Election Management System Election Event Designer Training	10 days		
D-Suite Accumulation only EMS Training	2 days		
D-Suite Results Tally & Reporting	1 day		
D-Suite ICP Training	1 day		
D-Suite ICX Training	1 day		
D-Suite ICC & Adjudication Training	1 day		
D-Suite UOCAVA Training	1 day		
D-Suite Mobile Ballot Printing Training	1 day		
Pollworker Train the Trainer	1 day		
Election Day Rover Training	0.5 days		
Poll Pad Train the Trainer	1 day		
Pollworker Training - Pilot			
Regional Training 1	67 days	Thu 8/1/19	Fri 11/1/19
D-Suite Accumulation only EMS Training	2 days		
D-Suite Results Tally & Reporting	1 day		
D-Suite ICP Training	1 day		
D-Suite ICX Training	1 day		
D-Suite ICC & Adjudication Training	1 day		
D-Suite UOCAVA Training	1 day		
D-Suite Mobile Ballot Printing Training	1 day		
Pollworker Train the Trainer	1 day		
Election Day Rover Training	0.5 days		
Poll Pad Train the Trainer	5 days		
Pollworker Training - Pilot			
Regional Training 2	67 days	Thu 8/1/19	Fri 11/1/19
D-Suite Accumulation only EMS Training	2 days		
D-Suite Results Tally & Reporting	1 day		
D-Suite ICP Training	1 day		
D-Suite ICX Training	1 day		
D-Suite ICC & Adjudication Training	1 day		
D-Suite UOCAVA Training	1 day		
D-Suite Mobile Ballot Printing Training	1 day		
Pollworker Train the Trainer	1 day		
Election Day Rover Training	0.5 days		
Poll Pad Train the Trainer	5 days		
Pollworker Training - Pilot			

Refresh Training	67 days	Thu 8/1/19	Fri 11/1/19
Election Programming - November 2019 General Election			
November 2019 General Election	1 day	Tue 11/5/19	Tue 11/5/19
Ballot Definition and Programming			
Data entry and import	5 days	Wed 8/7/19	Tue 8/13/19
Ballot Styling	1 day?	Wed 8/7/19	Wed 8/7/19
Review and modifications	1 day	Fri 9/6/19	Fri 9/6/19
Generate official ballots	15 days	Fri 9/6/19	Thu 9/26/19
Generate audio ballots	3 wks	Fri 9/6/19	Thu 9/26/19
Generate election files	3 wks	Fri 9/6/19	Thu 9/26/19
Generate test decks	2 wks	Fri 9/6/19	Thu 9/19/19
Ballot Production and L&A Testing			
UOCAVA Ballots Ready	1 day?	Sat 9/21/19	Sat 9/21/19
Official ballot printing	15 days	Sat 9/21/19	Thu 10/10/19
Logic and accuracy testing	15 days	Sat 9/21/19	Thu 10/10/19
Election Readiness			
Voter Outreach			
Pollworker Training	21 days	Mon 10/7/19	Mon 11/4/19
Equipment Delivery to Polls	6 days	Mon 10/28/19	Mon 11/4/19
Poll Pad Pilot Readiness			
Confirm iOS and application updates	5 days	Mon 9/30/19	Fri 10/4/19
Deploy application updates	10 days	Mon 10/7/19	Fri 10/18/19
Confirm ePulse settings	5 days	Mon 10/14/19	Fri 10/18/19
Load election data	5 days	Mon 10/21/19	Fri 10/25/19
Verify election data	1 day	Fri 10/25/19	Fri 10/25/19
Poll Pad Post Pilot Support			
Data Reconciliation	3 days	Wed 11/6/19	Fri 11/8/19
Export Data	1 day	Mon 11/11/19	Mon 11/11/19
Auditing the election	1 day	Tue 11/12/19	Tue 11/12/19
Archiving the elections	1 day	Wed 11/13/19	Wed 11/13/19
Phase 1 complete			
Phase 1 Lessons Learned Meeting	1 day	Tue 11/12/19	Tue 11/12/19
Phase 2 Installations			
Counties Receiving Equipment Phase 2 Part 1			
Election Management System			
Documentation Delivery			
Installation guides	0.25 days	Wed 11/6/19	Wed 11/6/19
User guides	0.25 days	Wed 11/6/19	Wed 11/6/19
Equipment			
Procurement and Delivery	40 days	Wed 11/6/19	Tue 12/31/19
Installation	40 days	Wed 11/6/19	Tue 12/31/19
County Level Acceptance Testing and Training	40 days	Wed 11/6/19	Tue 12/31/19
Tabulator and Accessible Voting System			
Documentation Delivery			
User Manuals	0.25 days	Wed 11/6/19	Wed 11/6/19
Quick reference guides	0.25 days	Wed 11/6/19	Wed 11/6/19
Maintenance manuals	0.25 days	Wed 11/6/19	Wed 11/6/19

Training manuals	0.25 days	Wed 11/6/19	Wed 11/6/19
Equipment	40 days	Wed 11/6/19	Tue 12/31/19
Procurement and Delivery	40 days	Wed 11/6/19	Tue 12/31/19
County Level Acceptance Testing and Training	40 days	Wed 11/6/19	Tue 12/31/19
Supplies and Consumables	40 days	Wed 11/6/19	Tue 12/31/19
Procurement and Delivery	40 days	Wed 11/6/19	Tue 12/31/19
Training			
Regional Training 1	40 days	Wed 11/6/19	Tue 12/31/19
D-Suite Accumulation only EMS Training	2 days		
D-Suite Results Tally & Reporting	1 day		
D-Suite ICP Training	1 day		
D-Suite ICX Training	1 day		
D-Suite ICC & Adjudication Training	1 day		
D-Suite UOCAVA Training	1 day		
D-Suite Mobile Ballot Printing Training	1 day		
Pollworker Train the Trainer	1 day		
Election Day Rover Training	0.5 days		
Poll Pad Pollworker Training	1 day		
Regional Training 2	40 days	Wed 11/6/19	Tue 12/31/19
D-Suite Accumulation only EMS Training	2 days		
D-Suite Results Tally & Reporting	1 day		
D-Suite ICP Training	1 day		
D-Suite ICX Training	1 day		
D-Suite ICC & Adjudication Training	1 day		
D-Suite UOCAVA Training	1 day		
D-Suite Mobile Ballot Printing Training	1 day		
Pollworker Train the Trainer	1 day		
Election Day Rover Training	0.5 days		
Poll Pad Pollworker Training	1 day		
Regional Training 3	40 days	Wed 11/6/19	Tue 12/31/19
D-Suite Accumulation only EMS Training	2 days		
D-Suite Results Tally & Reporting	1 day		
D-Suite ICP Training	1 day		
D-Suite ICX Training	1 day		
D-Suite ICC & Adjudication Training	1 day		
D-Suite UOCAVA Training	1 day		
D-Suite Mobile Ballot Printing Training	1 day		
Pollworker Train the Trainer	1 day		
Election Day Rover Training	0.5 days		
Poll Pad Pollworker Training	1 day		
Regional Training 4	40 days	Wed 11/6/19	Tue 12/31/19
D-Suite Accumulation only EMS Training	2 days		
D-Suite Results Tally & Reporting	1 day		
D-Suite ICP Training	1 day		
D-Suite ICX Training	1 day		
D-Suite ICC & Adjudication Training	1 day		
D-Suite UOCAVA Training	1 day		

D-Suite Mobile Ballot Printing Training	1 day		
Pollworker Train the Trainer	1 day		
Election Day Rover Training	0.5 days		
Poll Pad Pollworker Training	1 day		
Regional Training 5	40 days	Wed 11/6/19	Tue 12/31/19
D-Suite Accumulation only EMS Training	2 days		
D-Suite Results Tally & Reporting	1 day		
D-Suite ICP Training	1 day		
D-Suite ICX Training	1 day		
D-Suite ICC & Adjudication Training	1 day		
D-Suite UOCAVA Training	1 day		
D-Suite Mobile Ballot Printing Training	1 day		
Pollworker Train the Trainer	1 day		
Election Day Rover Training	0.5 days		
Poll Pad Pollworker Training	1 day		
Regional Training 6	40 days	Wed 11/6/19	Tue 12/31/19
D-Suite Accumulation only EMS Training	2 days		
D-Suite Results Tally & Reporting	1 day		
D-Suite ICP Training	1 day		
D-Suite ICX Training	1 day		
D-Suite ICC & Adjudication Training	1 day		
D-Suite UOCAVA Training	1 day		
D-Suite Mobile Ballot Printing Training	1 day		
Pollworker Train the Trainer	1 day		
Election Day Rover Training	0.5 days		
Poll Pad Pollworker Training	1 day		
Regional Training 7	40 days	Wed 11/6/19	Tue 12/31/19
D-Suite Accumulation only EMS Training	2 days		
D-Suite Results Tally & Reporting	1 day		
D-Suite ICP Training	1 day		
D-Suite ICX Training	1 day		
D-Suite ICC & Adjudication Training	1 day		
D-Suite UOCAVA Training	1 day		
D-Suite Mobile Ballot Printing Training	1 day		
Pollworker Train the Trainer	1 day		
Election Day Rover Training	0.5 days		
Poll Pad Pollworker Training	1 day		
Regional Training 8	40 days	Wed 11/6/19	Tue 12/31/19
D-Suite Accumulation only EMS Training	2 days		
D-Suite Results Tally & Reporting	1 day		
D-Suite ICP Training	1 day		
D-Suite ICX Training	1 day		
D-Suite ICC & Adjudication Training	1 day		
D-Suite UOCAVA Training	1 day		
D-Suite Mobile Ballot Printing Training	1 day		
Pollworker Train the Trainer	1 day		
Election Day Rover Training	0.5 days		

Poll Pad Pollworker Training	1 day		
Regional Training 9	40 days	Wed 11/6/19	Tue 12/31/19
D-Suite Accumulation only EMS Training	2 days		
D-Suite Results Tally & Reporting	1 day		
D-Suite ICP Training	1 day		
D-Suite ICX Training	1 day		
D-Suite ICC & Adjudication Training	1 day		
D-Suite UOCAVA Training	1 day		
D-Suite Mobile Ballot Printing Training	1 day		
Pollworker Train the Trainer	1 day		
Election Day Rover Training	0.5 days		
Poll Pad Pollworker Training	1 day		
Regional Training 10	40 days	Wed 11/6/19	Tue 12/31/19
D-Suite Accumulation only EMS Training	2 days		
D-Suite Results Tally & Reporting	1 day		
D-Suite ICP Training	1 day		
D-Suite ICX Training	1 day		
D-Suite ICC & Adjudication Training	1 day		
D-Suite UOCAVA Training	1 day		
D-Suite Mobile Ballot Printing Training	1 day		
Pollworker Train the Trainer	1 day		
Election Day Rover Training	0.5 days		
Poll Pad Pollworker Training	1 day		
Regional Training 11	40 days	Wed 11/6/19	Tue 12/31/19
D-Suite Accumulation only EMS Training	2 days		
D-Suite Results Tally & Reporting	1 day		
D-Suite ICP Training	1 day		
D-Suite ICX Training	1 day		
D-Suite ICC & Adjudication Training	1 day		
D-Suite UOCAVA Training	1 day		
D-Suite Mobile Ballot Printing Training	1 day		
Pollworker Train the Trainer	1 day		
Election Day Rover Training	0.5 days		
Poll Pad Pollworker Training	1 day		
Regional Training 12	40 days	Wed 11/6/19	Tue 12/31/19
D-Suite Accumulation only EMS Training	2 days		
D-Suite Results Tally & Reporting	1 day		
D-Suite ICP Training	1 day		
D-Suite ICX Training	1 day		
D-Suite ICC & Adjudication Training	1 day		
D-Suite UOCAVA Training	1 day		
D-Suite Mobile Ballot Printing Training	1 day		
Pollworker Train the Trainer	1 day		
Election Day Rover Training	0.5 days		
Poll Pad Pollworker Training	1 day		
Regional Training 13	40 days	Wed 11/6/19	Tue 12/31/19
D-Suite Accumulation only EMS Training	2 days		

D-Suite Results Tally & Reporting	1 day		
D-Suite ICP Training	1 day		
D-Suite ICX Training	1 day		
D-Suite ICC & Adjudication Training	1 day		
D-Suite UOCAVA Training	1 day		
D-Suite Mobile Ballot Printing Training	1 day		
Pollworker Train the Trainer	1 day		
Election Day Rover Training	0.5 days		
Poll Pad Pollworker Training	1 day		
Regional Training 14	40 days	Wed 11/6/19	Tue 12/31/19
D-Suite Accumulation only EMS Training	2 days		
D-Suite Results Tally & Reporting	1 day		
D-Suite ICP Training	1 day		
D-Suite ICX Training	1 day		
D-Suite ICC & Adjudication Training	1 day		
D-Suite UOCAVA Training	1 day		
D-Suite Mobile Ballot Printing Training	1 day		
Pollworker Train the Trainer	1 day		
Election Day Rover Training	0.5 days		
Poll Pad Pollworker Training	1 day		
Refresh Training	40 days	Wed 11/6/19	Tue 12/31/19
Phase 2 Part 1 Complete	0 days	Tue 12/31/19	Tue 12/31/19
Phase 2 Part 1 Wrap up Meeting			
Phase 2 Part 2 Installations	13 days	Wed 1/1/20	Fri 1/17/20
Counties Receiving Equipment Phase 2 Part 2	13 days	Wed 1/1/20	Fri 1/17/20
Election Management System	13 days	Wed 1/1/20	Fri 1/17/20
Documentation Delivery	1 day	Wed 1/1/20	Wed 1/1/20
Installation guides	0.25 days	Wed 1/1/20	Wed 1/1/20
User guides	0.25 days	Wed 1/1/20	Wed 1/1/20
Equipment	13 days	Wed 1/1/20	Fri 1/17/20
Procurement and Delivery	13 days	Wed 1/1/20	Fri 1/17/20
Installation	13 days	Wed 1/1/20	Fri 1/17/20
County Level Acceptance Testing and Training	13 days	Wed 1/1/20	Fri 1/17/20
Tabulator and Accessible Voting System	13 days	Wed 1/1/20	Fri 1/17/20
Documentation Delivery	1 day	Wed 1/1/20	Wed 1/1/20
User Manuals	0.25 days	Wed 1/1/20	Wed 1/1/20
Quick reference guides	0.25 days	Wed 1/1/20	Wed 1/1/20
Maintenance manuals	0.25 days	Wed 1/1/20	Wed 1/1/20
Training manuals	0.25 days	Wed 1/1/20	Wed 1/1/20
Equipment	13 days	Wed 1/1/20	Fri 1/17/20
Procurement and Delivery	13 days	Wed 1/1/20	Fri 1/17/20
County Level Acceptance Testing and Training	13 days	Wed 1/1/20	Fri 1/17/20
Supplies and Consumables	13 days	Wed 1/1/20	Fri 1/17/20
Procurement and Delivery	13 days	Wed 1/1/20	Fri 1/17/20
Presidential Preference Primary Election			Tue 3/24/20
Presidential Preference Primary Election	1 day	Tue 3/24/20	Tue 3/24/20
Presidential Preference Primary Lessons Learned	0 days	Wed 3/25/20	Wed 3/25/20

Election Programming			
Data entry and import	3 days	Wed 12/4/19	Fri 12/6/19
Ballot Styling	2 days	Wed 12/4/19	Thu 12/5/19
Review and modifications	2 days	Fri 1/3/20	Mon 1/6/20
Generate official ballots	2 days	Fri 1/3/20	Mon 1/6/20
Generate audio ballots	2 days	Fri 1/3/20	Mon 1/6/20
Generate election files	2 days	Fri 1/3/20	Mon 1/6/20
Generate test decks	2 days	Fri 1/3/20	Mon 1/6/20
Ballot Production and L&A Testing			
UOCAVA Ballots Ready	1 day?	Sat 1/18/20	Sat 1/18/20
Official ballot printing	15 days	Sat 1/18/20	Thu 2/6/20
Logic and accuracy testing	15 days	Sat 1/18/20	Thu 2/6/20
Election Readiness			
Voter Outreach			
Pollworker Training	21 days	Mon 2/3/20	Sat 2/29/20
Transport to polling	6 days	Mon 2/24/20	Mon 3/2/20
Poll Pad Election Readiness			
Confirm iOS and application updates	5 days	Mon 2/3/20	Fri 2/7/20
Deploy application updates	14 days	Mon 2/10/20	Thu 2/27/20
Confirm ePulse settings	5 days	Mon 2/17/20	Fri 2/21/20
Load election data	5 days	Mon 2/24/20	Fri 2/28/20
Verify election data	1 day	Fri 2/28/20	Fri 2/28/20
Poll Pad Post Election Support	7 days	Wed 3/25/20	Thu 4/2/20
Data Reconciliation	3 days	Thu 3/26/20	Mon 3/30/20
Export Data	1 day	Tue 3/31/20	Tue 3/31/20
Auditing the election	1 day	Wed 4/1/20	Wed 4/1/20
Archiving the elections	1 day	Thu 4/2/20	Thu 4/2/20
May Primary Election			Tue 5/26/20
May Primary Election	1 day	Tue 5/26/20	Tue 5/26/20
May Primary Election Lessons Learned	1 day	Wed 5/27/20	Wed 5/27/20
Election Programming			
Data entry and import	3 days	Wed 2/26/20	Fri 2/28/20
Ballot Styling	2 days	Wed 2/26/20	Thu 2/27/20
Review and modifications	2 days	Fri 3/27/20	Mon 3/30/20
Generate official ballots	1 day	Fri 3/27/20	Fri 3/27/20
Generate audio ballots	1 day	Fri 3/27/20	Fri 3/27/20
Generate election files	1 day	Fri 3/27/20	Fri 3/27/20
Generate test decks	1 day	Fri 3/27/20	Fri 3/27/20
Ballot Production and L&A Testing			
UOCAVA Ballots Ready	1 day?	Sat 4/11/20	Sat 4/11/20
Official ballot printing	15 days	Sat 4/11/20	Thu 4/30/20
Logic and accuracy testing	15 days	Sat 4/11/20	Thu 4/30/20
Election Readiness			
Voter Outreach			
Pollworker Training	21 days	Mon 4/27/20	Mon 5/25/20
Transport to polling	6 days	Mon 5/18/20	Mon 5/25/20
July Primary Election Runoff			Tue 7/28/20

June Primary Election	0 days	Tue 7/28/20	Tue 7/28/20
June Primary Runoff Lessons Learned	1 day	Wed 7/29/20	Wed 7/29/20
Election Programming			
Data entry and import	3 days	Wed 4/29/20	Fri 5/1/20
Ballot Styling	2 days	Wed 4/29/20	Thu 4/30/20
Review and modifications	2 days	Fri 5/29/20	Mon 6/1/20
Generate official ballots	1 day	Fri 5/29/20	Fri 5/29/20
Generate audio ballots	1 day	Fri 5/29/20	Fri 5/29/20
Generate election files	1 day	Fri 5/29/20	Fri 5/29/20
Generate test decks	1 day	Sat 6/13/20	Sat 6/13/20
Ballot Production and L&A Testing			
UOCAVA Ballots Ready	1 day?	Sat 6/13/20	Sat 6/13/20
Official ballot printing	15 days	Sat 6/13/20	Thu 7/2/20
Logic and accuracy testing	15 days	Sat 6/13/20	Thu 7/2/20
Election Readiness			
Voter Outreach			
Pollworker Training	21 days	Tue 6/30/20	Tue 7/28/20
Transport to polling	6 days	Mon 7/20/20	Mon 7/27/20
November 2020 General Election			Tue 11/3/20
November 2020 General Election	0 days	Tue 11/3/20	Tue 11/3/20
November 2020 General Election Lessons Learned	1 day	Wed 11/4/20	Wed 11/4/20
Election Programming			
Data entry and import	3 days	Wed 8/5/20	Fri 8/7/20
Ballot Styling	2 days	Wed 8/5/20	Thu 8/6/20
Review and modifications	2 days	Fri 9/4/20	Mon 9/7/20
Generate official ballots	1 day	Fri 9/4/20	Fri 9/4/20
Generate audio ballots	1 day	Fri 9/4/20	Fri 9/4/20
Generate election files	1 day	Fri 9/4/20	Fri 9/4/20
Generate test decks	1 day	Fri 9/4/20	Fri 9/4/20
Ballot Production and L&A Testing			
UOCAVA Ballots Ready	1 day?	Sat 9/19/20	Sat 9/19/20
Official ballot printing	15 days	Sat 9/19/20	Thu 10/8/20
Logic and accuracy testing	15 days	Sat 9/19/20	Thu 10/8/20
Election Readiness			
Voter Outreach			
Pollworker Training	21 days	Mon 10/5/20	Mon 11/2/20
Transport to polling	6 days	Mon 10/26/20	Mon 11/2/20
Project Closeout Meeting(s)	4 days	Tue 12/15/20	Fri 12/18/20

APPENDIX A TO ATTACHMENT 4 TO SOLUTION ORDER

Critical Milestones

Table A - Critical Milestones:	Milestone Deadline
1. Delivery and Acceptance of 2 ICX BMD units and 2 ICP scanners for public demonstrations and initial training	5 days after Agreement Effective Date
2. Delivery and Acceptance of Equipment and Software required to conduct the Pilot Election via the Solution, as mutually agreed to by the Parties	30 days after Agreement Effective Date
3. Delivery and Acceptance preliminary 10 ICX BMD units and 10 ICP scanners for public demonstrations and training	September 15, 2019
4. Delivery and Acceptance of all Democracy Suite Election management system hardware and software	October 15, 2019
5. Certification of the November 2019 Pilot Election conducted via the Solution.	November 22, 2019
6. Delivery and Acceptance of all remaining ImageCast Precinct Scanner Kits	December 31, 2019
7. Delivery and Acceptance of all remaining ImageCast Central Scanner Kits	December 31, 2019
8. Delivery and Acceptance of all electronic pollbook Kits	December 31, 2019
9. Delivery and Acceptance of all remaining ImageCast X BMD Kits	January 15, 2020
10. Delivery and Acceptance of all remaining ancillary items	January 31, 2020
11. Certification of the March 24, 2020 Presidential Preference Primary conducted via the Solution.	April 10, 2020
12. Certification of the November 3, 2020 General Election conducted via the Solution	November 20, 2020

RETRIEVED FROM DEMOCRACYDOCKET.COM

ATTACHMENT 5 TO SOLUTION ORDER

RESERVED

RETRIEVED FROM DEMOCRACYDOCKET.COM

ATTACHMENT 6 TO SOLUTION ORDER

Training Plan

Georgia Implementation Training Plan

The following is an in-depth training plan as requested and is submitted with the understanding that training dates and training content are subject to change pending award of the contract and the outcome of collaboration with the GASOS/County Election Officials.

Pre-Training Tasks

2 Days: 7/30 to 7/31 - Meeting with GASOS and GASOS-selected County Election Officials to customize training documentation, syllabi, demonstration project and ballots to reflect GA election procedures and terminology.

11 Days: 8/1 to 8/11 - Customized training documentation, syllabi, demonstration project and ballot development.

Phase 1 Training Plan

GASOS – 8/12 to 8/23 – 11 1/2 Days. During this period, GASOS review and approval of final training documentation, syllabi, demonstration project and ballot and set/confirm the training schedule.

- Election Programming – 4 1/2 Days
- DSuite Administrator and User – 2 Days
- ICX-BMD/ICP Operator – 1 Day
- ICC/ADJ Administration – 1 Day
- ICC/ADJ Operator – ½ Day
- UOCAVA – 1 Day
- Election day Rover Training – ½ day
- Pollpad Train the Trainer Training – 1 day

Counties – Administrative/User – 8/26 to 9/9 – 2 Regional Trainings - 4 Days Each

- DSuite Administrator and User – 2 Days
- ICC/ADJ Administration – 1 Day
- UOCAVA – 1 Day

Counties – Operator/Pollworker – 9/10 to 9/13 – 2 Regional Trainings - 3 Days Each

- ICX-BMD/ICP Operator – 1 Day
- ICC/ADJ Operator – ½ Day
- Pollworker Train the Trainer – ½ Day
- Pollpad Training – 1 day

Phase 2 Training Plan

Counties not holding December Runoff Election

Counties – Administrative/User – 11/11 to 12/13 – Regional Trainings - 4 Days Each

- DSuite Administrator and User – 2 Days
- ICC/ADJ Administration – 1 Day
- UOCAVA – 1 Day

Counties – Operator/Pollworker – 11/11 to 12/13 – Regional Trainings - 3 Days Each

- ICX-BMD/ICP Operator – 1 Day
- ICC/ADJ Operator – ½ Day
- Pollworker Train the Trainer – ½ Day
- Pollpad Training – 1 day

Counties holding December Runoff Election

Counties – Administrative/User – 12/9/2019 to 1/17/2020 – Regional Trainings - 4 Days Each

- DSuite Administrator and User – 2 Days
- ICC/ADJ Administration – 1 Day
- UOCAVA – 1 Day

Counties – Operator/Pollworker – 12/9/2019 to 1/17/2020 – Regional Trainings - 3 Days Each

- ICX-BMD/ICP Operator – 1 Day
- ICC/ADJ Operator – ½ Day
- Pollworker Train the Trainer – ½ Day
- Pollpad Training – 1 day

Courses

DSuite Election Programming – 4.5 Days

- Democracy Suite Election Programming Software Overview
- Template (Master) Election Project Concepts
- Election Programming Phases
- Introduction to Election Event Designer
- Election Project Definition – Primary and General Elections
- Divisioning – Districts, Precincts, and Elector and Ballot Groups
- Election Event – Contests and Candidates
- User Management
- Advancing to Election Project Styling
- Ballot Styling and Templates
- Translations – Single and Multiple Language
- Creating the Ballots and Audio Ballot Files
- Previewing Audio Ballot Files
- Creating Electronic Ballot Headers
- Tabulation Setup

- Preparing Proofing Packages
- Create Election (Tabulator) Files
- Create Final Project Backup for Transfer to County
- Advanced Functions – Creating Template (Master) Projects and Using Election Data Translator for Import/Export of Election Definition Data

DSuite Administrator and User – 2 ½ Days

- Introduction to Democracy Suite
 - Democracy Suite Software Component Overview
 - Tabulator Systems Overview
 - ImageCast Precinct Ballot Scanner – ICP
 - ImageCast X-Ballot Marking Device – ICX-BMD
 - ImageCast Central – ICC
 - Review of Quick Reference Guides
 - Additional System Components
 - Consumable Items
 - Voting System Process Overview
 - Generic Election Timeline and Workflow Responsibilities Review
- The Election Proofing Process
 - Overview of the County Proofing Process
 - The Election Proofing Package
 - Proofing Ballots
 - Proofing Reports
 - Proofing Audio Ballot Files
- Election Preparation
 - Election Event Designer – EED – Programming the Tabulators
 - Setting Up ImageCast Central – ICC
 - Setting Up Adjudication
- Logic and Accuracy Testing
 - Testing Steps Overview
 - Test Deck Overview
 - Logic and Accuracy Test Procedures
 - ICX-BMD/ICP
 - ICC with Adjudication
 - RTR
- Results Talley and Reporting - RTR
 - Overview of RTR
 - Opening an Election in RTR
 - RTR Settings
 - Loading Election Results
 - Managing Results Files and Tabulators in RTR
 - Manual Entry of Results
 - Results Reporting and Exporting
 - Exporting Results Manually
- Backing up the Final Results
- Purging Test Results

ICX-BMD/ICP Operator – 1 Day

- ICP Operations
 - Hardware Overview
 - Loading/Changing Paper Tape
 - Loading the Memory Cards
 - Acceptance Testing
 - Maintenance and Troubleshooting
- ICX-BMD Operations
 - Hardware Overview
 - Loading Paper and Toner in the BMD Printer
 - Loading Election Files
 - Acceptance Testing
 - Maintenance and Troubleshooting
- Logic and Accuracy Testing
 - Test Decks and Vote Sims
- Voting Equipment in the Polling Place
 - Setting up the Equipment
 - Opening the Polls
 - Activating Voter Cards
 - Voting on the ICX-BMD/ICP
 - Closing the polling place

ICC/ADJ Administration – 1 Day

- Overview of ICC and ADJ Functionality
- Setting Up the ICC – Loading the Tabulator Files and Scanner Configuration
- Setting Up RTR to Manage, Monitor and Automatically Upload Results From ICC/ADJ
- Setting Up Adjudication – Loading the Election and Setting Conditions
- Logic and Accuracy Testing
- Ballot Handling
 - Scanning Ballots and Common problems
 - Batch Handling
 - Rejecting and Resetting batches
 - Deleting Batches
- Adjudicating Ballots
 - Standard User Vs. Administrative User
 - Ballot Overlays
 - Ballot Review and AuditMark
 - Write-in Resolution
 - Submitting Batches
 - Managing Quarantined Ballots
 - Configuring and Managing Report Profiles

ICC/ADJ Operator – ½ Day

- Ballot Handling
 - Scanning Ballots and Common problems
 - Batch Handling
 - Rejecting, Resetting, and Deleting Batches
- Adjudicating Ballots
 - Ballot Overlays

- Ballot Review and AuditMark
- Write-in Resolution
- Quarantining Ballots

UOCAVA – 1 Day

- Configuring UOCAVA
 - Display
 - Language Management
 - Voter ID and PIN Options
- Tabulator Management
 - Importing Election Files
 - Configuring Parameters
- Download Administration
 - Editing the Ballot Package
 - Cover Sheet, Affidavit, and Return Envelope Settings
 - Security Question Administration
- User Management
- Customization
 - Logos
 - Color Schemes
- Voter List Management
- Accessibility
- Testing
- Reporting

Election Day Rover Training – 1 Day

- Preparing for Election Day
- Opening and Closing the polls
- Processing Voters
- Assisting Voters with Special Needs
- Troubleshooting Election Day Problems

Pollpad Train the Trainer Training – 1 Day

- ePulse training
 - Create elections
 - Administer elections
 - Closing out elections
 - Monitoring pollpads
 - Generating reports
- Train the trainer
 - Set up of pollpad solution
 - Familiarizations of screens, statuses, and functionality
 - Configuration
- Meraki Mobile Device Management System training
 - Enrolling pollpad
 - Updating pollpad applications
 - Ensuring proper restriction settings
 - Monitoring/remote wipe devices

Pollworker Train the Trainer – ½ Day

- Training Techniques
- Learning Styles
- Presentation Skills
- Voting Equipment in the Polling Place
 - Setting up the Equipment
 - Opening the Polls
 - Activating Voter Cards
 - Voting on the ICX-BMD/ICP
 - Troubleshooting
 - Closing the Polls

RETRIEVED FROM DEMOCRACYDOCKET.COM

Exhibit C

To Master Solution Purchase and Services Agreement

FORM OF SERVICES ORDER

THIS SERVICES ORDER ("**Services Order**") is dated this _____ day of _____, 20__ ("**Services Order Effective Date**") and is subject to the terms of the Master Solution Purchase and Services Agreement (the "**Agreement**") dated as of _____, 20109 by and between _____ ("**State**") and _____ ("**Contractor**"). Unless otherwise defined herein, all capitalized terms used herein have the same meanings as is set forth in the Agreement, which is hereby incorporated by reference. The undersigned State Entity hereby orders delivery for the following pieces of Solution from Contractor. Contractor agrees to deliver the items ordered herein in accordance with the Agreement and in compliance with all Applicable Laws including with the provisions of O.C.G.A. Title 21, as amended and the State of Georgia Election Board and Secretary of State Rules contained in Sections 183 and Sections 590 of the Georgia Administrative Code respectively.

NOW, THEREFORE, in consideration of the mutual covenants and conditions contained herein, State and Contractor hereby agree as follows:

In performing Services under this Services Order, Contractor shall communicate to _____ of State or his/her designee

DESCRIPTION OF THE SERVICES.

Project Overview. The <insert project name here> project ("**Project**") is <insert descriptive summary of the project associated with these services>.

Services Order Purpose. The purpose of this Services Order is for Contractor to provide the following services <insert a short general descriptive summary> to State related to the Project.

Services Scope. Contractor is responsible for the following Services and scope, as further described and detailed below, in the context of the overall Project:

<Please provide a list of services to be performed by Contractor here. If the services are subject to any specific specifications, requirements or acceptance criteria, please list them here.>

SCHEDULE.

Contractor shall complete the Services and provide any Deliverables on or before _____. The parties agree that time is of the essence in this Agreement.

<Please provide a schedule here, including a commencement date, a completion date, and any interim milestone dates.>

DESCRIPTION OF DELIVERABLES.

<Please provide a list of deliverables here, including a delivery date for each of the deliverables. If the deliverables are subject to any requirements or acceptance criteria, please list them.>

MILESTONES

Contractor shall deliver to Company the Deliverables listed in the table below during the period of performance of this Services Order.

Item Number	Deliverables / Milestone	Due Date	Final Acceptance Criteria
1.	<Identify all "items" (including interim deliverables) that will be developed or provided as a result of contractor performing the tasks detailed in Section Error! Reference source not found. above (i.e., products, plans, status reports, documentation, etc.)>	XX/XX/XX	<Describe the precise conditions / criteria that will be applied to determine that the Deliverable is accepted for payment issuance to the Contractor>.
2.			

FEES AND EXPENSES.

The Fees for the Services shall not exceed [redacted], and [Expenses associated with performing the Services shall not exceed [redacted].]

Any additional services shall be set forth in an additional Statement of Work executed by STATE and Contractor under the Agreement or in a purchase order issued by STATE and accepted by Contractor under the Agreement. Contractor shall be reimbursed for additional reasonable expenses if pre-approved by STATE in writing.

DEVIATIONS FROM TERMS OF AGREEMENT

[Insert any deviations from the Master Agreement]

This Services Order is approved by:

STATE OF GEORGIA

OFFICE OF THE SECRETARY OF STATE

DOMINION VOTING SYSTEMS, INC.

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Exhibit D

To Master Solution Purchase and Services Agreement

LIST OF PERMITTED CONTRACTOR SOLUTION PARTNERS

1. KNOWiNK, LLC having its principal place of business at 2111 Olive Street, Saint Louis, MO 63103.
2. Diversified Technologies, LLC having its principal place of business at 100 Peachtree St, Atlanta, GA 30303.

RETRIEVED FROM DEMOCRACYDOCKET.COM

Exhibit E

To Master Solution Purchase and Services Agreement

CHANGE CONTROL FORM

RETRIEVED FROM DEMOCRACYDOCKET.COM

1. Contract Information. This change control form is provided pursuant to and governed by Section 6.2 of the Master Solution Purchase and Services Agreement entered into between State and Contractor as of _____ (“Agreement”). Any term used but not defined in this Change Control Form will have the meaning given to it in the Agreement. Once this Change Control Form is signed by both parties below it shall be deemed a Change Order.

Contract Control No.	Change Order No.	For Solution Order or Services Order No.
-----------------------------	-------------------------	---

2. Party Information.

Name Of Requesting Party:	Name of Party to whom Submitted:	Date Submitted:

3. Change Request. (Attach additional pages referencing this Section as required.)

Change to: (identify one only)	Description of Requested Change
<input type="checkbox"/> Deliverable <input type="checkbox"/> Services Task	

4. Impact Analysis. (Required to be filled-out with all Change Requests submitted by Contractor and as part of all Change Responses returned to State by Contractor as part of a State submitted Change Requests. Attach additional pages referencing this Section as required.)

Resource Impact:	
Cost Impact:	
Timing Impact:	
Date Response Delivered	

5. Change Response - Acceptance or Rejection of Change Request.

HAVING RECEIVED, UNDERSTOOD AND AGREED with this Change Control Form, (check only one) STATE Contractor hereby (initial one):

_____ accepts the Change Request and desires to proceed with the change requested hereon.

_____ rejects the Change Request and does not desire to proceed with the change requested hereon and hereby terminates such request.

6. Change Order. If this Change Control Form is signed by both parties below it shall be deemed a Change Order and shall become a part of the Solution Order or Services Order to which it relates, shall be governed by this Agreement and shall be attached thereto as if initially entered into as part of a Solution Order or Services Order.

State ENTITY	CONTRACTOR
_____	_____
AUTHORIZED SIGNATURE & DATE SIGNED	AUTHORIZED SIGNATURE & DATE SIGNED

<hr/> PRINTED NAME & TITLE	<hr/> PRINTED NAME & TITLE
-------------------------------	-------------------------------

RETRIEVED FROM DEMOCRACYDOCKET.COM

Exhibit F

To Master Solution Purchase and Services Agreement

RESERVED

RETRIEVED FROM DEMOCRACYDOCKET.COM

Exhibit G

To Master Solution Purchase and Services Agreement

FEE SCHEDULE

First Year Purchase Summary - Prices of equipment, technical facilities, software, and other related services for voting, vote counting, and result processing. All pricing in U.S. Dollars.

DESCRIPTION	QTY	TOTAL GROUP COST
Central Scanning Solution: Absentee / Central Count		
ImageCast Central Kit - G1130	14	
ImageCast Precinct Tabulator (Absentee Only without ballot box)	153	
Sub-Total:		\$816,768.00
In-Person Voting Solution: Ballot Marking Device		
ImageCast X Kit - Prime	30050	
ImageCast X BMD Polling Place Metal Cart	30050	
ATI Kit - ICX - USB	2754	
Polling Place UPS	2750	
Sub-Total:		\$59,684,408.50
In-Person Voting Solution: Precinct Scanner/Tabulator		
ImageCast Precinct Tabulator	3500	
ImageCast Precinct Ballot Box - Plastic	3500	
ICP Paper Roll (98')	14000	
Seals - Pull Up / Pull Tight - Plastic - Red (25/pkg)	1120	
Seals - Pull Quick (25/pack)	560	
Seals - Tamper Evident Security Label (25/pkg)	5368	
Sub-Total:		\$8,156,260.00
In-Person Voting Solution: Electronic Pollbook Hardware and Software		
EPB Unit (Apple IPAD)	8,000	
Carrying Case (without printer)	8,000	
Stand	8,000	
Stylus	16,000	
Encoders	8,000	
Isync Drives	2,800	
EPB Software Initial License	8,000	
Administrative Dashboard/Command Center and Reporting	1	
Sub-Total:		\$5,671,440.00
Election Management Hardware and Software		
EMS Standard Server Kit	14	
EMS Client Workstation Kit	151	
EED/RTR/ Adjudication Workstation Kit	28	
Smart UPS 1500 (rack mountable for Standard Server)	14	
Smart UPS 1500 (non-rack mountable for Express Server)	151	
Democracy Suite Standard Initial License (through 12/31/2021)	1	
Adjudication Module Initial License (through 12/31/2021)	1	

Automated Test Deck Module Initial License (through 12/31/2021)	1	
Remote UOCAVA Module Initial License (through 12/31/2021)	1	
Sub-Total:		\$834,673.35
Support Services	Days	
Implementation and Training		
Product Implementation & Support	510	
Project Management & Implementation	1716	
Logic & Accuracy Testing	640	
Training (/day)	320	
Train The Trainer: Poll worker	28	
Democracy Suite Full System Training	20	
Democracy Suite Result, Tally and Reporting	80	
ImageCast Central Operator Training	80	
ImageCast Central Adjudication Training (reserved)	80	
ImageCast Precinct Training	80	
Election Setup / Ballot Setup	1045	
On-site Services - Election Day	1280	
On-Site Services - Non-Election Day (/day)	200	
Sub-Total:		\$14,772,040.80
Purchase - Year 1 Total:		\$89,935,590.65
BMD security paper ballots	\$0.13/ballot	TBD

Annual Purchase Summary - Dominion shall provide invoices for Annual Licenses and Warranties on January 1 of each Term year. Dominion shall provide invoices for BMD ballot security paper upon delivery to the State for each Election during the Term. The State shall pay invoices in a timely manner in accordance with the terms of the Agreement. All pricing in U.S. Dollars.

Ballot Marking Device Security Paper		
BMD security paper ballots	\$0.13/ballot	TBD

Annual Software Licenses: 2022		
Democracy Suite Standard Annual License Fee	1	\$190,500.00
Adjudication Annual License Fee	1	Included
Automated Test Deck Annual License Fee	1	Included
Remote UOCAVA Module Annual License Fee	1	Included
Electronic Poll Book Management System Annual License Fee	1	Included
Electronic Poll Book (EPoll) Annual License Fee	8000	Included
ImageCast X Annual License Fee	30050	\$2,319,108.00
ImageCast Precinct Annual License Fee	3653	\$410,571.00
ImageCast Central Annual License Fee	14	\$287,605.50
TOTAL:		\$3,207,784.50

Annual Software Licenses: Years 2023 - 2029		
Democracy Suite Standard Annual License Fee	1	\$190,500.00
Adjudication Annual License Fee	1	Included
Automated Test Deck Annual License Fee	1	Included
Remote UOCAVA Module Annual License Fee	1	Included
Electronic Poll Bool Management System Annual License Fee	1	Included
Electronic Poll Book (EPoll) Annual License Fee	8000	Included
ImageCast X Annual License Fee	30050	\$1,660,342.00
ImageCast Precinct Annual License Fee	3653	\$293,637.00
ImageCast Central Annual License Fee	14	\$205,114.00
TOTAL:		\$2,349,593.00

Annual Warranty: 2022 (optional to county)		
Electronic Poll Book (EPoll) Annual License Fee	8000	\$890,000.00
ImageCast X Annual License Fee	30050	\$2,396,412.38
ImageCast Precinct Annual License Fee	3653	\$1,498,522.62
ImageCast Central Annual License Fee	14	\$67,656.75
TOTAL:		\$4,852,591.75

Annual Warranty: Years 2023 – 2029 (optional to county)		
Electronic Poll Book (EPoll) Annual License Fee	8000	\$890,000.00
ImageCast X Annual License Fee	30050	\$1,593,886.00
ImageCast Precinct Annual License Fee	3653	\$997,483.00
ImageCast Central Annual License Fee	14	\$47,515.00
TOTAL:		\$3,528,884.00

Price List – Standard Price List without volume discounts for future purchases by counties.

ImageCast Central Kit - G1130	\$25,000.00
ImageCast Central Kit - M160ii	\$7,500.00
ImageCast X Kit - Prime	\$3,500.00
ImageCast X Prime Voter Smart Card - Generic	\$8.10
ImageCast X Prime Poll Worker Smart Card - Generic	\$8.10
ImageCast X Prime Technician Smart Card - Generic	\$8.10
ImageCast Precinct Tabulator - 320C	\$3,900.00
Mobil Ballot Printing Kit #2 Portable High Volume	\$5,800.00
EMS Standard Server Kit (R630/WS2012/SS2016)	\$17,000.00
EMS Client Workstation Kit	\$1,700.00
EMS Adjudication Workstation Kit	\$1,700.00
Smart UPS 1500 (rack mountable)	\$800.00
ATI Kit - ICX - USB	\$375.00
ImageCast X Voting Booth - Standard	\$295.00

ImageCast X Prime Transport Bag - Single	\$60.00
ImageCast X BMD Printer Transport Bag	\$63.00
ImageCast Precinct Ballot Box - Plastic	\$1,000.00
ICP Paper Roll (98')	\$4.00
Seals - Pull Up / Pull Tight - Plastic - Red (25/pkg)	\$14.00
Seals - Pull Quick (25/pack)	\$6.75
Seals - Tamper Evident Security Label (25/pkg)	\$16.75

RETRIEVED FROM DEMOCRACYDOCKET.COM

Exhibit H

To Master Solution Purchase and Services Agreement

INSURANCE

A. PERFORMANCE BOND

Contractor shall furnish a performance bond or an irrevocable letter of credit to the State for the faithful performance of the Agreement in an amount equal to 100% of the value of the Agreement as determined by the State. The bond shall be issued by a Corporate Surety authorized to do business with the State of Georgia. The performance bond/letter of credit must be submitted to the State within ten (10) calendar days of the date the Agreement is awarded, but in any event, prior to the beginning of any contract performance by the Contractor. The Performance Bond requirement shall expire on December 31, 2020.

B. MINIMUM INSURANCE COVERAGE

- 1.1 Workers' Compensation and Employer's Liability - Statutory Workers Compensation as required by the laws of all jurisdictions (other than the State of Georgia) in which Contractor Personnel are physically present to perform the Services and/or the premises at which such Services were performed, and Employers' Liability with a minimum limit of not less than \$1 Million per occurrence. In the State of Georgia, Contractor shall maintain Workers Compensation Insurance (Occurrence) in the amounts of the statutory limits established by the General Assembly of the State of Georgia. Any self-insurer must submit a certificate from the Georgia Board of Workers Compensation stating that the supplier qualifies to pay its own workers compensation claims. In addition, Contractor shall require all subcontractors occupying the premises or performing work under the Agreement to obtain an insurance certificate showing proof of Workers Compensation Coverage with the following minimum coverage:
- Bodily injury by accident - per employee \$100,000;
 - Bodily injury by disease - per employee \$100,000; and
 - Bodily injury by disease – policy limit \$500,000.
- 1.2 Commercial General Liability (CGL) - On a per occurrence basis, including (a) products / completed operations coverage; (b) independent contractors protective coverage; and (c) contractual liability coverage, which coverage must specifically cover Contractor's indemnification provisions contained herein (but net of intellectual property indemnification which shall be covered by the policies required in Section 1.5 below). The CGL policy must be maintained in effect for ten (10) years following the date of expiration or termination of the Agreement. The CGL policy shall provide for the following minimum coverage.
- Each Occurrence Limit - \$1,000,000;
Personal & Advertising Injury Limit - \$1,000,000;
 - General Aggregate Limit - \$2,000,000; and
 - Products/Completed Ops. Aggregate Limit - \$2,000,000.
- 1.3 Automobile Liability - Covering all non-owned and hired vehicles utilized in the performance of the Agreement with a combined single limit of not less than \$1 Million per occurrence (inclusive of amounts under Contractor's umbrella policy).
- 1.4 Professional Errors & Omissions – Coverage, which shall include, but not be limited to, loss or damage resulting from errors and omissions, advertising injury, personal injury (including invasion of privacy), intellectual property offenses related to software, internet, network and e-business activities, claims of code misappropriation, code theft, copyright and/or trademark infringement with an aggregate limit of no less than \$3 Million per claim. If the policy is issued on a claims-made basis, either an extended reporting period of not less than ten (10) years following the expiration or

termination of the Agreement shall be provided; or such coverage must be maintained in effect for ten (10) years following the date of expiration or termination of the Agreement. The retroactive date shall not precede the (signature) date of the Agreement.

- 1.5 Commercial Fidelity and Crime Insurance – Coverage with a limit of not less than \$1,000,000 per occurrence, including coverage for or the benefit of State in the event of loss of money, securities or property third party legal liability, or fraud arising out of or in connection with the acts or omissions of Contractor Personnel in an amount not less than \$1 Million per loss.
- 1.6 Cyber-Liability Insurance - Coverage \$1,500,000 per occurrence covering liability for transmission of a virus, hacker damage, theft or unauthorized disclosure of private information, theft of digital ID, cyber business interruption, cyber extortion, and consumer and client coverage.
- 1.7 Excess or Umbrella Liability Insurance - Coverage on a follow-form basis, with a minimum limit of \$5,000,000 per occurrence and \$5,000,000 as an annual aggregate, in excess of the following insurance coverages described above: Worker’s Compensation Insurance and Employer’s Liability Insurance coverage; Commercial General Liability Insurance; and Automobile Liability Insurance coverage.

RETRIEVED FROM DEMOCRACYDOCKET.COM

Exhibit I

To Master Solution Purchase and Services Agreement

FORM OF DELIVERY & ACCEPTANCE NOTICE

RETRIEVED FROM DEMOCRACYDOCKET.COM



On-Site Acceptance Test Checklist ICX Prime – ImageCast X®

COUNTY: _____

DATE: _____

MODEL: _____

SW VERSION: _____

SERIAL NUMBER: _____

STEP NO.	STAGE DESCRIPTION	DETAILS	PASS ✓	COMMENTS <i>Please list any anomalies or issues and resolution.</i>
Unpacking & Inspection Stage				
1		Ensure the system is properly packed.		
2	Physical Inspection	Ensure that the following items are present in the packaging box: <ol style="list-style-type: none"> 1. Inspect the machine for any external damage. 2. Inspect the screen 3. Inspect the stand 4. Inspect the card reader slot 5. Open the four external doors and check for damage to ports. 6. Verify the presence of the power cord(10') and the external battery 		
3		Place ICX and HP Printer on flat surface		
4	Hardware Setup	Connect AC Power Supply to ICX (bottom-right corner)		
5		Connect Power Cable to rear of HP Printer		
Power Up and System Status Verification (with Test CF cards)				
	Maintenance Diagnostic	Turn on Printer (Front of Unit)		
		Turn on ICX Prime(bottom-right door)		
		ICX unit launches the ICX application by default		
		Check battery charging status (top right tool bar)		
Verify Android Version/Kernel Version				
	Maintenance Diagnostic (Continue)	Insert Technician Card: <ol style="list-style-type: none"> 1. Enter Technician Pin and Select Login 2. Confirm and modify the date and time 3. Select Android Settings 4. Select About Tablet 5. Verify Android Version 6. Verify Kernel Version Date 7. Select home 		
		Check functionality of all USB ports: <ol style="list-style-type: none"> A. Unplug ATI cable from USB port and plug into each USB port not being use. B. There are a total of 6 ports: 4 ports inside top left door, 2 ports inside top right door. C. Light blinks when plugged in. Repeat for each USB port. D. When finished, plug ATI cable back into original USB port 		
	Functional Testing	Load Elections Files On USB (PG ICX.dat file) Load Election file to ICX: <ol style="list-style-type: none"> 1. Insert Technician card 2. Enter Technician Pin and Select Login 3. Select Load Election Data 4. Select the PG_ICX.dat file 5. Select the select option 6. Select Copy 7. Select OK 8. Select Result Location to Prime (Drop down menu) 9. Select Apply 10. Select OK 11. Remove Technician Card 		
	Functional Testing (Continue)	Open Election Polls: <ol style="list-style-type: none"> 1. Insert Pollworker Card 2. Enter Pollworker Pin and Select Login 3. Select the appropriate tabulator (Drop down menu) 4. Select OK 5. Check the box to enable AVS Controller 6. Check the box to enable Manual Session Activation 7. Select Yes 8. Select OK 9. Remove Pollworker Card 		

		<p>Activate a Manual Voter Session:</p> <ol style="list-style-type: none"> 1. Insert Pollworker card 2. Select the Activation Ballot tab 3. Enter Activation Code 4. Select Next 5. Select Regular 6. Voting Session will start 7. Remove Pollworker card 		
		<p>Activate a Manual Voting Session with Audio:</p> <ol style="list-style-type: none"> 1. Insert pollworker Card 2. Select the Activation Ballot tab 3. Select Enable AVS controller check box 4. Select Next 5. Select Regular 6. Voting Session will start, LED will turn yellow 7. Remove Pollworker Card 		
		<p>Vote and cast Audio ballot:</p> <ol style="list-style-type: none"> 1. Select Vote in English 2. Select ATI 3. Make Voting selections with ATI and cast ballot 4. Confirm selections are heard on headphone 5. Select more (top right corner) 6. Cancel Activation 		
		<p>Vote and Cast Ballot:</p> <ol style="list-style-type: none"> 1. Select Vote in English 2. Make voting selections and cast ballot 3. Print ballot, confirm printed selections 4. Insert ICX ballot into ICP2 Tabulator 5. Confirm ICP2 has accepted ICX Ballot 		
		<p>Close polls:</p> <ol style="list-style-type: none"> 1. Insert Pollworker card 2. Enter Pollworker Pin and select Login 3. Select Close poll and select yes 4. Report Prints 5. Select OK 6. Remove Pollworker card 		
		<p>Re-zero results:</p> <ol style="list-style-type: none"> 1. Insert Technician card 2. Enter Technician pin and select Login 3. Select Re-zero 4. Select Yes 5. Re-enter Technician pin 6. Confirm all results are deleted 7. Select OK 		
		<p>Reset Machine:</p> <ol style="list-style-type: none"> 1. Select Clear All Election Data 2. Select Yes 3. Enter Technician pin 4. Confirm selections are heard on headphone 5. Confirm all election data, results and audit logs are deleted 6. Select OK 		
		Power off Unit (bottom right corner)		



Acceptance Test Checklist ImageCast® Precinct

County: _____

DATE: _____

PCOS MODEL: _____

FW VERSION: _____

PCOS SERIAL NUMBER: _____

STEP NO.	STAGE DESCRIPTION	DETAILS	P A S S ✓	COMMENTS <i>Please list any anomalies or issues and resolution.</i>
Unpacking & Inspection Stage				
1	Unpacking	Ensure the system is properly packed in a large plastic zip-tight bag.		
2		Ensure that the following items are present in the packaging box: 1. Power supply unit 2. Power Cord. 3. Two (2) Memory Cards 4. Two (2) Security Keys (iButtons)		
3		Verify that the ICP is secured to the ballot box correctly.		
4		Verify unit has external doors installed and function correctly.		
5	Inspection	Ensure that there are no obvious scratch marks, dents or spots.		
Power Up and System Status Verification (with Test cards)				
6	System Power Up Status Verification	Insert two (2) cards programmed with a Test Election Project into the memory card slots of the tabulator. Note: The Test Election Project must be compatible with the SW installed on the tabulator.		
7		Power up the system and verify that the appropriate audio-visual indications are seen and heard and that the correct F/W version successfully installed.		
8		When prompted by the operator screen (accompanied by an audible beep), place the security token on the tabulator. Hold the token in place until the operator screen displays "Key Accepted, Validating Election Files"		
Functional Testing (with Test Election cards) <small>(Note: This section is to be performed based on the ImageCast® L1 Tech Guide v0-02 20160310 Level 1 Maintenance Manual)</small>				
9		Select "Utilities" from the Admin menu. Select "Diagnostic" from the Utilities menu and select "Complete" and verify that all diagnostic functions complete successfully		
10		Verify that the printed tape has the same serial number that is on the tabulator and also has the correct software version listed		
11	Election Project Testing	Select the "open Poll" option from the Administrator menu. The Operator Screen will display that the totals are zero. Press the "Zero" button to print the zero proof.		
12		Inspect the printed tape to verify that the serial number on the tape matches the tabulator.		
13		Unplug the A/C power from the rear of the unit to verify that the unit is running on battery.		
14		Perform standard voting using the supplied test deck. Note: This is not a conclusive battery capacity test but only verification of the battery's ability to hold charge. Re-Connect to AC power source upon completion.		
15		Close the polls and print the results tape. Verify that the results on the report match the expected results as per the Master Results Report Tape .		
16		Re-zero the memory cards.		
17		Follow the standard procedure to power down the tabulator.		
18	Power Down & Sign	Unplug AC power cord and any peripheral devices attached to the tabulator.		
19		Record the machine Serial Number in the Inventory Database.		
20		Place the completed and signed Checklist with the tabulator.		
21		Store the system away or set aside for dispatch, whichever required.		
22				



On-Site Acceptance Test Checklist ICC – Canon ImageCast Central®

COUNTY: _____

DATE: _____

MODEL: _____

SW VERSION: _____

SERIAL NUMBER: _____

STEP NO.	STAGE DESCRIPTION	DETAILS	PASS	COMMENTS <i>Please list any anomalies or issues and resolution.</i>
Unpacking & Inspection Stage				
1	Unpacking	Ensure the system is properly packed.		
2		Ensure that the following items are present in the packaging box: 5. Power cord 6. USB Data cable 7. Dell all in one workstation 8. Keyboard, mouse, power cord, dell driver disk 9. CF card reader, iButton reader and adaptor		
3		Ensure there are no loose screws or parts.		
4		Remove all tape and foam packaging from scanner and workstation.		
5	Inspection	Ensure that there are no obvious scratch marks, dents or spots.		
6		Verify that the Scanner, keyboard, mouse, iButton reader and CF card reader are all plugged into the workstation properly.		
Power Up and System Status Verification (with Test CF cards)				
7	System Power Up	Insert one (1) CF card programmed with a Test Election Project into the CF reader and attach the iButton to the Iwire adaptor.		
8		Power up the system, Enter the login credentials and verify that the operating system powers up correctly and no hardware error messages occur.		
Functional Testing (with Test Election CF cards)				
9	Election Project Testing	Load the election files to the proper location as specified in the ICC user guide.		
10		Verify the following: 10. Open the ICC Application and enter the administrator code "12345678" 11. Ensure that the scanner initializes and no error messages occur. 12. Verify the Software version of the application under the "Status" tab.		
11		Under Configuration: 1. Enter supervisor mode and verify that the scan options are set to maximum paper length and that the driver options are set to user guide saved profile. 2. Set the server path if applicable 3. Change stop options if applicable		
12		Print or save a zero proof report from the status menu.		
13		Scan the pre marked test deck and verify that the scanner is stopping on all exception ballots that were pre-determined.		
14		Close the tabulator and print or save the results report.		
15		Compare Results to the master report for accuracy.		
16		Power Down & Sign	Zero the tabulator and close the application.	
17	Reset the DVS folder to a new election state by deleting the all election files from the DVS and config folders and power down the scanner.			

Exhibit J

To Master Solution Purchase and Services Agreement

DISASTER RECOVERY PLAN

Overview

The Disaster Recovery & Business Continuity Plan (“DRCP”) described herein details the coordinated mitigation strategies employed by Dominion Voting Systems, Inc. (Dominion) during project implementation in conjunction with the State of Georgia in the event of a disaster leading to business interruptions

This Plan remains valid until superseded by a revised DRCP mutually endorsed by the partners. This DRCP outlines the parameters of all strategies offered as the primary partners mutually understand them. This DRCP does not supersede current processes and procedures unless explicitly stated herein.

Dominion will from time to time review its procedures with respect to security safeguards through risk assessments, benchmarking or other means, to determine whether they are still consistent with applicable Privacy Laws, appropriate to the risks, and consistent with best practices, and if not, Dominion will revise the same as required.

Scope and Objectives

The scope of this Disaster Recovery & Business Continuity Plan is to document the coordination and support strategies set by the State of Georgia in conjunction with Dominion in the event of a disaster or major business interruption. Dominion shall implement the recovery strategies as set forth in this document in line with the State of Georgia processes.

The objectives of the Disaster Recovery & Continuity Plan include the following:

- To minimize interruptions of normal operations.
- To limit the extent of disruption and damage.
- To minimize the economic impact of the interruption.
- To establish alternative means of operation in advance.
- To train personnel with emergency procedures.
- To provide smooth and rapid restoration of service.

The Disaster Recovery & Continuity Plan accounts for a variety of disruption types. The first step is to identify the potential disaster and issue types and assess the risk associated with each one. After identifying the potential risks, it is necessary to grade them based on likelihood and seriousness. Preventative measures are then identified for risk prevention and recovery strategies are outlined in cases where disruption occurs.

Team Members & Responsibilities by Phase

This disaster recovery plan focuses on the primary Crisis Team and departmental/management leadership responsibilities related to incidents or situations outside normal business operations. The Crisis Team will include both senior GASOS and Dominion management (President, Executive Vice Presidents and local Project Manager) and specific corporate department heads (Accounting, Administration/Facilities, Human Resources, Information Technology, and Marketing and Sales). The Dominion Executive Vice President and GASOS designated executive (or other senior GASOS assigned staff) may designate additional staff from their areas of responsibility to assist the Crisis Team. This may be particularly important if a location other than the main corporate headquarters in Denver, CO or our Atlanta metro

area facility is impacted by a disaster situation. In a situation of this nature, the local Project Manager and his/her department heads will assist the Crisis Team with any additional support required provided by wither Dominion or GASOS corporate offices.

At Imminent Declaration of a Disaster

Crisis Team

- All Crisis Team members must work to ensure the immediate safety and well-being of all GASOS, Dominion staff, and electors present.
- Implement the Disaster Recovery & Business Continuity Plan (DRCP).
- Adjust the task list and timelines of the DRCP as necessary.
- The GASOS Crisis Team members in collaboration with Dominion Crisis Team members will communicate with all staff, insurance and service providers customers, news media as necessary (via telephone, email, fax, or through local cable or radio channels – employees should follow local guidelines regarding radio or cable channels to monitor in case of a disaster situation in their area.)
- The President of Dominion, with informational assistance from both GASOS and Dominion staff, will make the decision regarding “Stay and Repair”, “Repair and Temporarily Relocate”, or “Permanently Relocate” operations.
- Monitors DRCP progress.
- Assists each employee/department as required
- The President of Dominion in partnership with the designated executive from GA SOS is responsible for making the decision regarding when to transition from the crisis phase to the recovery phase of the plan.
- Implement Recovery Phase tasks.
- GASOS in partnership with Dominion will communication with staff, insurance and service providers, customers, news media as necessary.
- The President of Dominion and the designated executive from GASOS are responsible for making the decision regarding when the recovery phase has been completed and the corporation can return to “business as usual.”
- Critique and review DRCP and processes and update and enhance the DRCP as needed.
- Dissemination of updated DRCP/destruction of previous version of DRCP.

Senior Management

- Remain visible to employees, customers, and stakeholders.
- Delegate recovery roles.
- Establish the Disaster Recovery as a partnership between GASOS and Dominion
- Direct, manage and monitor the recovery.
- Ensure all business and operational units receive normal ongoing support (offices and business units in other locations not impacted by the disaster).
- Avoid the temptation to participate “hands on.”
- Publicly praise success.
- Rationally amend business plans/projections as necessary.
- Closely control media and analyst communications to ensure accuracy of information dissemination.

Human Resources

- Monitor employee morale
- Monitor productivity of personnel
- Prioritize reallocation of resources
- Provide appropriate retraining
- Provide counseling and support resources

Technology Management

- Identify/prioritize mission critical applications
- Prepare business impact analysis by unit
- Re-assess original recovery plans as necessary
- Continuously assess recovery site stability
- Recover/reconstruct all critical data ASAP in the agreed order (department, function, site, etc.)
- Ensure all business and operational units receive normal ongoing support (offices and business units in other locations not impacted by the disaster)
- Information systems security during the disaster and recovery, including opportunistic fraud

Within the Recovery Environment

Crisis Team

- Assesses the adequacy of information security
- Assesses the adequacy of system security
- Re-assesses recovery tolerance/timeframes
- Evaluates recovery contingencies
- Develops and tests recovery plans semi-annually
- Develops emergency plans for recovery staff
- Evaluates Information systems security

Customers Clients and Suppliers

- Re-establishes customer and vendor contacts ASAP
- Recover/reconstructs customer data and contracts
- Continues full customer support/assistance services
- Reconsider product and service cost/delivery projections

In the Post-Disaster Environment

Crisis Team

- Assists in responses to any changed customer requirements
- Assesses ability to respond to customer requests/inquiries
- Assesses Customer/Counterparty stability
- Assesses Supplier/Vendor reliability
- Statuses existing orders and contracts
- Assists in fulfillment of Customer support needs

Finance Department, General Counsel and Compliance

- Protect facilities from further damage
- Site security
- Formally notify insurers of any claims
- Ensure all business and operational units receive normal ongoing support (offices and business units in other locations not impacted by the disaster)

Process Re-Establishment

- Key reconciliations
- Other financial controls
- Meaningful key performance indicators

Dominion Operations

- Assess ability to deliver customer orders
- Identify outsourcing options/opportunities
- Refresh supply chain management
- Analyze lease options/requirements
- Establish new risk Dominion controls
- Amend policies and procedures
- Monitors DRCP progress assists each employee/department as required
- Implement Recovery Phase tasks continue communication with staff, insurance and service providers, customers, and other items
- Critique and review DRCP and processes and update and enhance the DRCP as needed
- Dissemination of updated DRCP/destruction of previous version of DRCP

Identification of Disaster Scenarios

The types of disasters that we must prepare for include the following:

- Environmental disasters
- Criminal disasters
- Hardware failures
- Programming and Generation Failures
- Service and Shipping Failures
- Network and Power Failures

Environmental and Criminal Disasters

Environmental disasters can range from events such as fires and floods. To account for these types of potential disasters, Dominion incorporates preventative measures into the initial project plan. Although the likelihood of these types of disasters is low, the seriousness is quite high. Dominion maintains inventories of spare voting equipment (both vote counters and accessible voting devices) in case of such disasters. In addition to spare equipment and systems, Dominion also maintains an inventory of spare parts that can be used to repair systems with minor damage.

In the event of an Environmental Disaster, the recovery strategy includes deployment of spare units to the affected voting locations. This additional equipment may be used to supplement the project, if the scope of the disaster is far worse than the spare units are capable of rectifying. The recovery strategy for a criminal disaster would also include deploying spare units and replacing the units through investigative and insurance claims.

Security systems and/or secure storage facilities are used to store spare inventory and Dominion requires that the customer implement similar security measures when responsible for voting equipment and hardware. Dominion equipment also incorporates built-in security features on each other their voting unit through the use of redundant memory media locks, and seal hasps.

All edges, upon which a tabulator is connected to the ballot box, are pre-sealed in manufacturing to prevent ballots from being dropped within the ballot box without passing through the vote center. These edges can further be sealed with the use of sticker seals.

Hardware Failures

Although there is a higher likelihood of hardware failures, than environmental or criminal disasters, these types of failures are commonly less serious or severe. Hardware failures encompass any type of issue that may prevent the use of the vote counting equipment or accessible voting equipment.

Preventative measures are employed on all equipment in order to minimize the potential for hardware failures. These measures include diagnostic testing and maintenance prior to deployment. The maintenance and diagnostic testing examines the condition of the equipment and its components and tests the systems hardware and configuration. Diagnostic testing examines the functionality of the equipment and ensures all aspects are in proper working order.

Dominion maintains inventories of spare voting equipment (both vote counters and accessible voting devices) in case of such disasters. In addition to spare equipment and systems, Dominion also maintains an inventory of spare parts that can be used to repair systems with minor damage. Supplementary units are deployed in the event of a major hardware failure, and their initial inclusion in the project plan is another preventative measure for this type of failure.

Prior to an election event, pre-election logic and accuracy testing is performed. Similar to the preventative testing implemented by Dominion, logic and accuracy testing ensures accurate functioning of the equipment. Any malfunctions or deficiencies found during L&A testing can be repaired in advance of the election event. If a hardware failure of any type occurs, the recovery strategy would include troubleshooting, and diagnosis. If the failure is deemed non-repairable, a spare unit will be deployed in its place. Spare units should be included in the stock purchased by the GASOS so they are available for immediate deployment in regional deployment centers. This rapid deployment provides a solution to a hardware failure.

ID	Description of Risk	Preventative Measures	Recovery Strategy
1	Vote Counting Equipment: Malfunctions during tabulation/scanning	Diagnostic testing Pre-election Logic and Accuracy testing	Deploy spare voting units
2	Vote Counting Equipment: Malfunction during ballot review, prior to ballot being cast	Diagnostic testing Pre-election Logic and Accuracy testing	Deploy spare voting equipment
3	Accessible Voting Equipment: Malfunctions during accessible session (technical or user error)	Diagnostic testing Pre-election Logic and Accuracy testing	Deploy spare voting equipment
4	Accessible Voting Equipment: Malfunctions during review of voting session, prior to paper ballot printing	Diagnostic testing Pre-election Logic and Accuracy testing	Deploy spare voting equipment

5	Accessible Voting Equipment: Malfunction during ballot printing	Diagnostic testing Pre-election Logic and Accuracy testing	Deploy spare voting equipment
6	Voting Equipment: Malfunctions during opening or closing of polls	Diagnostic testing Pre-election Logic and Accuracy testing	Deploy spare voting equipment
7	Voting Equipment: Malfunctions during advance or special voting days	Diagnostic testing Pre-election Logic and Accuracy testing	Deploy spare voting equipment
8	Voting Equipment: Malfunctions during pre-election Logic and Accuracy testing	Diagnostic testing	Deploy spare voting equipment
9	Voting Equipment: Malfunctions during post-election Logic and Accuracy testing	Diagnostic testing Pre-election Logic and Accuracy testing	Deploy spare voting equipment

Programming and Configuration Failures

Programming and configuration failures are most likely to occur during the configuration phase (pre-election). Preventative measures include testing configurations and programming prior to delivery to the customer. For example, ballots are tested after printing to ensure that the voting equipment is able to gather the appropriate information from the ballot. These testing steps are implemented so if an error is discovered they can be corrected as part of the recovery strategy. The recovery strategy for this type of failure, involves determining the error and rectifying it immediately. The preventative steps are put in place, so errors can be detected and the recovery strategy may be implemented in a timely manner.

ID	Description of Risk	Preventative Measures	Recovery Strategy
10	Error during memory card and security key programming	Tested prior to being sent to {client name}	Determine error and correct; reprogram cards
11	Unable to collect pronunciation of candidate and party names through normal process	Software/Process already been used in the past to collect this info	Determine error and correct
12	Ballots generated incorrectly	Tested prior to printing	Determine error and correct
13	Ballots printed incorrectly	Tested after being printed	Determine error and correct; reprint ballots

Service and Shipping Failures

Please refer to the Service Level Agreement for detailed preventative measures and recovery strategies regarding the services provided by Dominion. Additional resources are available and factored in to the project plan for every Dominion project. In the event of a resource or delivery issue, for example, an employee taking leave during a project, additional resources are available

to supplement the project and in turn to prevent or recover from a resource issue. All Dominion employees utilize the same standardized procedures and collaboration techniques to ensure a seamless transition in case of accident or other business continuity threat.

ID	Description of Risk	Preventative Measures	Recovery Strategy
14	Model and Demonstration Units unavailable by requested Dates	Voting Equipment already manufactured and in- stock	Use Allotted Additional Resources
15	System equipment not shipped by time set out in the Project Plans	Voting Equipment already manufactured and in- stock Have used same shipping company for past elections;	Use Allotted Additional Resources
16	Supplies not delivered to correct location/by time set out in the Project Plans/ contract agreement	Most Supplies already manufactured and in- stock Have used same shipping company for past elections;	Use Allotted Additional Resources
17	Error in shipping results in system equipment not arriving at appropriate location	Have used same shipping company for past elections; never encountered this issue	Send another shipment with different shipping company
18	Shipment handling resulting in damage to system equipment	Have used same shipping company for past elections; never encountered this issue	Send another shipment with different shipping company
19	Unable to supply personnel for on- site support	Always schedule back-up personnel for on-site support	Use Allotted Additional Resources
20	Unable to perform training on date set out in Election Calendar	Always schedule back-up personnel for on-site training	Use Allotted Additional Resources
21	Issue in travel resulting in trainer unable to make training date/location	Never encountered this issue in past elections; always schedule travel ahead of training session to prevent these issues	Use Allotted Additional Resources

Power Failures

In the event of a power failure, the voting equipment is configured to maintain the integrity of Election Day results. The battery power supplied to the vote tabulator provides sufficient time to properly power-down the unit and protect the integrity of the results. If the battery discharges prior to a proper power-down, the results will remain stored in the memory cards, unchanged by the improper power down.

ID	Description of Risk	Preventative Measures	Recovery Strategy
24	Power failure resulting in call center being unreachable	Ensure other support locations are available	Route all calls and communications to alternate support location
25	Call center overloaded/network failure resulting in delay in return of calls/unreachable	Ensure other support locations are available	Route calls and communications to alternate support location
26	Network Failure during Ballot Generation	Generate Copies	Deploy Copy
27	Power Failure during Ballot Generation	Generate Copies	Deploy Copy
28	Power Failure on Election Day	Backup Battery in Voting Equipment	Shut down voting equipment. Use auxiliary port on ballot box.

Escalation Process

Contact Details

In the event of any type of disaster, the Vendor Delivery Manager will be the primary point of contact. The primary contact will have access to key resources on the Dominion Project teams as well as product and technical specialists and will be responsible for coordination of all recovery strategies.

Escalation Chain of Command

If during the recovery period the primary contact is not available, the following Dominion representatives should be contacted in the listed order below:

- Primary Contact:** Project Manager
- Secondary Contact:** Executive Sponsor
- Tertiary Contact:** President of Dominion Voting

From: David Moreno
Sent: Wednesday, February 5, 2020 12:36 AM
To: Ivan Vukovic; Dana LaTour; Sheree R. Noell
Cc: Nick Ikonomakis; Aamer Chaudhry; Eric Coomer
Subject: Re: AK - Legislation review -- access to database [EXTERNAL] Can you look at this and let me a good counter to it.

Are we overthinking this?

Legally speaking the Json exports could be considered a Database, which they can provide unencrypted.

DAVID MORENO | DIRECTOR, PRODUCT STRATEGY
DOMINION VOTING

1201 18th Street, Suite 210, DENVER, CO 80202

[REDACTED] | DOMINIONVOTING.COM
[REDACTED]
[REDACTED]

From: Ivan Vukovic [REDACTED]
Sent: Tuesday, February 4, 2020 4:59 PM
To: Dana LaTour; Sheree R. Noell; David Moreno
Cc: Nick Ikonomakis; Aamer Chaudhry
Subject: Re: AK - Legislation review - access to database [EXTERNAL] Can you look at this and let me a good counter to it.

From an engineering perspective, the main reason why we don't want unencrypted databases is that then the integrity of the election data and results cannot be guaranteed.

I've included David because he may be able to provide a more appropriate response with better wording for the customer.

I.

Get [Outlook .for iOS](#)

From: Aamer Chaudhry [REDACTED]
Sent: Tuesday, February 4, 2020 6:42:27 PM
To: Dana LaTour [REDACTED] Sheree R. Noell [REDACTED]
Cc: Ivan Vukovic [REDACTED]
Subject: RE: AK - Legislation review -- access to database [EXTERNAL] Can you look at this and let me a good counter to it.

I have copied **Ivan Vukovic**, he should be able to provide response to this or get someone who can.

Thanks,
Aamer

From: Dana LaTour [REDACTED]
Sent: February 4, 2020 6:34 PM
To: Sheree R. Noell [REDACTED]; Aamer Chaudhry [REDACTED]
Subject: AK - Legislation review -- access to database [EXTERNAL] Can you look at this and let me a good counter to it.

Sheree,

Gail is asking us to provide her with talking points to explain why access to the unencrypted database is a bad idea/ or not possible. Who should I reach out to? First thought is Eric, but he's on vacation. Kay? But she needs an answer ASAP.

Dana

From: Fenumiai, Gail M (GOV) [REDACTED]
Sent: Tuesday, February 4, 2020 3:29 PM
To: Dana LaTour [REDACTED]; William Mast [REDACTED]
Subject: [EXTERNAL] Can you look at this and let me a good counter to it.

I am trying to provide some comments for an amendment to a bill. I was prepared to state that we can provide precinct by precinct information, and we currently do, in a variety of electronic formats.

"* Sec. 2* AS 15.20 is amended by adding a new section to read:

Sec. 15.20.223. Provision of electronic database con-
state election. Regardless of whether an election recur
AS 15.20.430 or an election is contested under AS 15.20.540,
candidate, a political party, or an organization or organized ,
opposes an initiative, referendum, or recall at an election, the
without charge access to the unencrypted electronic database
tabulations and vote totals for the election."

Gail Fenumiai
Director, Division of Elections
Office of the Lieutenant Governor
[REDACTED]

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 800-57³ 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


Notary Public

My Commission Expires:

My Commission Expires 05/21/2028


Clay U. Parikh

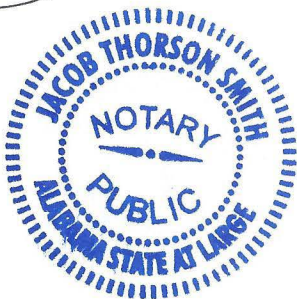


Exhibit A

RETRIEVED FROM DEMOCRACYDOCKET.COM

FROM [Appling Nov 2020 General [REDACTED]].[dbo].[[REDACTED]]

100 %

Results Messages

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

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]]

100 %

Results Messages

	description	RijndaelKey	RijndaelVector	X509Data	HMACKey
1	Bibb County November 2020 General and Special El...	Ka1& [REDACTED]	6E [REDACTED]	0x308205E10201 [REDACTED]	1A0... 0x326B7 [REDACTED]

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]]

100 %

Results Messages

description	RijndaelKey	RijndaelVector	X509Data	HMACKey
1 Jones County November 2020 General and Special E...	9"Td [REDACTED]	w^6J5 [REDACTED]	0x308205E10201 [REDACTED]	0x346 [REDACTED] 43678

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]]

100 %

Results Messages

description	RijndaelKey	RijndaelVector	X509Data	HMACKey
1 Telfair County November 2020 General and Special...	Ww [REDACTED] DP 2v	7a X [REDACTED] 3h	0x308205E10201 [REDACTED]	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

RETRIEVED FROM DEMOCRACYDOCKET.COM

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	JdKofUEZuB[REDACTED]JNFOMHVSRRGxg+a	Appling
Admin	0xC97922[REDACTED]A6A2EF52	State of	Georgia	dNEhq/8FJTp[REDACTED]D9GmlzPJqBjww+	Appling
Techadvisor	0x6B69EC[REDACTED]7C2ECDFC2	State of	Georgia	UdKofUEZuB[REDACTED]JNFOMHVSRRGxg+a	Bibb
Admin	0x6B69EC[REDACTED]7C2ECDFC2	State of	Georgia	dNEhq/8FJTp[REDACTED]D9GmlzPJqBjww+	Bibb
Techadvisor	0xC7A4C7[REDACTED]5D753F6B5	State of	Georgia	UdKofUEZuB[REDACTED]JNFOMHVSRRGxg+a	Jones
Admin	0xC7A4C7[REDACTED]5D753F6B5	State of	Georgia	dNEhq/8FJTp[REDACTED]D9GmlzPJqBjww+	Jones
Techadvisor	0x08A131[REDACTED]A8319A7B	State of	Georgia	UdKofUEZuB[REDACTED]JNFOMHVSRRGxg+a	Telfair
Admin	0x08A131[REDACTED]A8319A7B	State of	Georgia	dNEhq/8FJTp[REDACTED]D9GmlzPJqBjww+	Telfair
Techadvisor	0x6166A7[REDACTED]EF986384	John	Smith	UdKofUEZuB[REDACTED]JNFOMHVSRRGxg+a	Maricopa
Admin	0x7058D7[REDACTED]BE5984C2B	Bruce	Hoenicke	dNEhq/8FJTp[REDACTED]D9GmlzPJqBjww+	Maricopa
Techadvisor	0x6166A7[REDACTED]EF986384	John	Smith	UdKofUEZuB[REDACTED]JNFOMHVSRRGxg+a	Mesa
Admin	0x6166A7[REDACTED]EF986384	John	Smith	dNEhq/8FJTp[REDACTED]D9GmlzPJqBjww+	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:



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 now¹. 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.

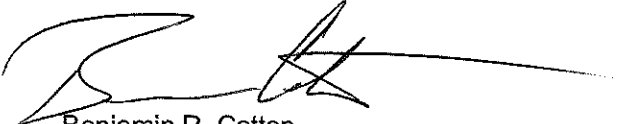
¹ There is no public acknowledgement or announcement that any modifications or updates have been made to the Dominion Democracy Suite 5.5A acquired by Georgia and used in the 2020 elections.

- 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.

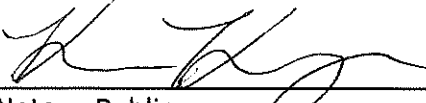
CONCLUSION

- 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

State of Washington

County of Kittitas

Signed and sworn to (or affirmed) before me on
8/18/24 by Keanna Krueger

Notary Public



RETRIEVED FROM DEMOCRACYDOCS

Sunday, August 25, 2024 at 20:38:47 Eastern Daylight Time

Subject: RE: SEB 2024-039: Benjamin Cotton
Date: Thursday, April 11, 2024 at 10:22:57 AM Eastern Daylight Time
From: McGowan, Charlene
To: Kurt Olsen
CC: Koth, Sara, Brunson, Michael, T. A. Harding, J.D., Blanchard, Joshua, Archie, Glenn
Attachments: image001.jpg

External [REDACTED]

[Report This Email](#) [FAQ](#) [Agio Phishing Protection](#)

Mr. Olsen,

Thank you for the information you provided and for speaking with our investigators. I understand that Mr. Cotton will make himself available for an interview if the scope is limited to his declaration statement that he forensically examined Dominion voting system components in Bibb County, Georgia. We can agree to limit the scope of the interview to his examination of components and/or documents in Bibb County, Georgia and not any other jurisdictions.

Please let me know if you'd like to discuss further. Otherwise, I trust you will make arrangements for the interview with our investigators.

Sincerely,
Charlene

Charlene S. McGowan

*General Counsel
Georgia Secretary of State*



From: Kurt Olsen [REDACTED]
Sent: Thursday, March 28, 2024 12:27 PM
To: McGowan, Charlene [REDACTED]
Cc: Koth, Sara [REDACTED]; Brunson, Michael [REDACTED]; T. A. Harding, J.D.

Subject: SEB 2024-039: Benjamin Cotton

EXTERNAL EMAIL: Do not click any links or open any attachments unless you trust the sender and know the content is safe.

Dear Ms. McGowan,

Todd A. Harding and I represent Ben Cotton with respect to the above-referenced investigation described in the email you sent yesterday to Andrew Parker. Please direct any further communications regarding Mr. Cotton to Todd and me.

In your email to Mr. Parker, you state that:

On March 11, 2024, Mr. Cotton signed a sworn declaration under penalty of perjury stating that he “forensically examined Dominion Voting Systems components in Maricopa County Arizona, Antrim County Michigan, Fulton County Pennsylvania, and Bibb County Georgia.” Your client previously signed a sworn declaration stating that he had forensically examined voting equipment in Coffee County, Georgia--not Bibb County. Our investigators reached out to you for an explanation for this discrepancy and were told that Mr. Cotton reviewed information he received from Bibb County in response to a FOIA request. However, this is contradictory to his sworn testimony that he “forensically examined [voting system] components”

Your belief that there is a “discrepancy” in Mr. Cotton’s declaration caused by Mr. Cotton’s use of the phrase “forensic examination” in connection with the word “components” in connection with the Bibb County electronic election record data produced pursuant to an Open Records Request is incorrect. Webster’s dictionary defines the adjective “forensic” as applied to e.g., an “examination” as follows: “belonging to, used in, or suitable to courts of judicature or to public discussion and debate.” Webster’s dictionary also defines “component” as simply “a constituent part.” Here, with respect to Bibb County, the individual hardware and software packages function together to produce a system. The backup election database is a “component” of the voting system. Bibb County produced the backup election database in connection with an Open Records Request more than two years ago. That backup election database was also posted on the web. See the Bib-recount.7z file at <https://www.zebraduck.org/election-files/georgia2020-11-03/ballot-images/>.

The Bibb County backup election database, which is public data, is precisely what Mr. Cotton forensically examined. An election database is a “component” of the election system. There is no “discrepancy” in Mr. Cotton’s sworn testimony.

Lastly, the findings described in Mr. Cotton’s declaration regarding Dominion Voting Systems, Inc.’s failure to protect the election encryption and decryption keys placed in the election database is a grave threat to Georgia’s (and other states’) election systems. As Mr. Cotton stated in his declaration, with these keys, a malicious inside actor or a non-insider can alter votes and vote tallies without detection. I am also attaching the

sworn Declaration of Clay Parikh who opined on this issue. Among Mr. Parikh's many cyber-related qualifications, Mr. Parikh conducted security tests on vendor voting systems for EAC certification of voting systems on behalf of Pro V&V from 2008 to 2017. Mr. Parikh further described Dominion's placing of these master cryptographic encryption keys unprotected on the election database (other than a Windows log-in which is easily bypassed) and in plain text is "an egregious, inexcusable violation of long-standing, basic security practices" and [Federal Information Processing Standards] FIPS—with which Dominion purports its encryption complies." See Parikh Dec. at ¶¶ 48-52. We stand ready to assist the Georgia Secretary of State's office with any investigation of this issue which we believe must be remedied before the 2024 election cycle to ensure the integrity of those election results.

All the best,

Kurt Olsen


Kurt B. Olsen
OLSEN LAW, P.C.
1250 Connecticut Ave., NW, Ste. 700
Washington DC 20036
(202) 408-7025
ko@olsenlawpc.com

The information in this transmittal may be legally privileged, confidential, and/or otherwise protected by law from disclosure, and is intended only for the recipient(s) listed above. If you are neither the intended recipient(s) nor a person responsible for the delivery of this transmittal to the intended recipient(s), you are hereby notified that any distribution or copying of this transmittal is prohibited. If you have received this transmittal in error, please notify Olsen Law P.C. immediately by return e-mail and take the steps necessary to delete it completely from your computer system. Thank you.