

Exhibit B

1 Mary R. O'Grady, 011434
2 Joshua D. Bendor, 031908
3 Emma J. Cone-Roddy, 034285
4 OSBORN MALEDON, P.A.
5 2929 North Central Avenue
6 21st Floor
7 Phoenix, Arizona 85012-2793
8 (602) 640-9000
9 mogrady@omlaw.com
10 jbendor@omlaw.com
11 econe-rodgy@omlaw.com

12 Attorneys for Secretary of State Katie Hobbs

13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

IN THE SUPERIOR COURT OF THE STATE OF ARIZONA

IN AND FOR THE COUNTY OF MARICOPA

ARIZONA DEMOCRATIC PARTY, an
Arizona political party and political action
committee; and STEVE GALLARDO, a
qualified elector,

Plaintiffs,

vs.

KAREN FANN, in her official capacity as
President of the Arizona Senate;
WARREN PETERSEN, in his official
capacity as Chairman of the Senate
Judiciary Committee; KEN BENNETT, in
his official capacity as the liaison of the
Arizona Senate; and CYBER NINJAS,
Inc., a Florida corporation,

Defendants.

No. CV2021-006646

**DECLARATION OF RYAN
MACIAS**

I, RYAN MACIAS, declare as follows:

1. I am over 18 years of age and am competent to testify regarding the matters discussed in this declaration.
2. My areas of expertise include election technology, security, and policy.
3. I have been retained in this matter to provide an expert opinion regarding the security and reliability of the practices and procedures of the Arizona Senate and

1 Cyber Ninjas, Inc. in their audit of the Maricopa County ballots and election equipment
2 from the 2020 General Election. I am not being compensated for my work in this case.

3 4. My *curriculum vitae* is attached to this report as **Exhibit 1**.

4 **EXPERT CREDENTIALS**

5 5. I am the owner of RSM Election Solutions LLC, an election technology
6 and cybersecurity consulting and advising company organized in Washington, D.C.,
7 registered as a foreign LLC in Oklahoma, and operating out of Tulsa, Oklahoma. RSM
8 Election Solutions LLC's core principle is: Resiliency in the election infrastructure =
9 Securing election technology + Mitigating risk to the democratic process.

10 6. I am a subject matter expert with over 15 years of experience in election
11 technology, security, and policy. In this capacity, I have developed strategies and advise
12 the election community, including federal, state, local, and tribal governments, on ways
13 to build resiliency in the election infrastructure. I engage directly with election officials
14 to identify risks to the election infrastructure and processes, as well as highlight
15 mitigative measures, compensating controls, and best practices that election officials
16 and private sector partners can implement to manage the risks. Previously, I was the
17 Acting Director of the U.S. Election Assistance Commission's ("EAC") Voting System
18 Testing and Certification Program, where I was the lead on modernizing the Voluntary
19 Voting System Guidelines ("VVSG"), version 2.0,¹ which focus on ensuring all voting
20 systems used in U.S. elections are secure, accurate, and accessible. Prior to that, I
21 served as the Senior Election Technology Program Specialist at the EAC for three years.
22 Prior to joining the EAC, I spent 10 years with the California Secretary of State's
23 Office, developing and implementing legislation, policies, and procedures on election
24 technology and security, including serving as the technology lead for the Post-Election
25

26
27
28

¹ [https://www.eac.gov/sites/default/files/eac_assets/1/6/VVSGv_2_0_Scope-Structure\(DRAFTv_8\).pdf](https://www.eac.gov/sites/default/files/eac_assets/1/6/VVSGv_2_0_Scope-Structure(DRAFTv_8).pdf)

1 Risk-Limiting Audit Pilot Program from 2011 to 2013.² For the November 3, 2020,
2 General Election, I also served as an expert, observing the hand count audit and recount
3 in Fulton County, Georgia.

4 7. In preparing this declaration, I reviewed the Complaint and related filings
5 in the following action: Arizona Democratic Party, et al. vs. Karen Fann, et al. in the
6 Superior Court of the State of Arizona in and for the County of Maricopa, Case No.
7 CV2021-006646. I have also conducted a search for and reviewed publicly available
8 material related to this matter, including the Cyber Ninjas, Inc. Master Services
9 Agreement (attached hereto as Exhibit 2) and Statement of Work (attached hereto as
10 Exhibit 3) for this audit and the Senate’s January 12, 2021 subpoena to Maricopa
11 County for election materials. I also was present at the Arizona Veterans Memorial
12 Coliseum, the location that the Arizona Senate procured for the recount portion of the
13 audit, on Thursday, April 22, 2021, to review the set-up, configuration, security
14 protocols, as well as the delivery of ballots. Further, I viewed the live video feed of the
15 Cyber Ninjas operation at the Coliseum, at <https://arizonaaudit.com/>, and a recording of
16 the April 22, 2021 press conference where Ken Bennett, the Senate’s audit liaison, and
17 Doug Logan, the CEO of Cyber Ninjas, Inc., provided information and answered
18 questions about the audit. My opinions below are based on my experience and expertise
19 in election technology, security, and policy and my review of these materials, video
20 feeds, and facility.

21 **I. Opinion 1: Neither the software nor hardware used by Cyber Ninjas**
22 **to scan the ballots for the Vote Count and Tally Phase have complied**
23 **with federal certification standards nor Arizona Title 16**
24

25
26
27 _____
28 ² <https://www.sos.ca.gov/elections/ovsta/frequently-requested-information/post-election-auditing-regulations-and-reports/post-election-risk-limiting-audit-pilot-program-2011-2013>

1 **requirements – specifically Arizona 16-442³ - including as to**
2 **accuracy, reliability, and security.**

3 8. In 2002, Congress passed the Help America Vote Act of 2002, Pub.
4 L.107-252, 116 Stat. 1666, (Oct. 29, 2002) ⁴ (“HAVA”) to improve the administration
5 of federal elections, including by providing minimum standards for voting machines.
6 *See, e.g.*, 52 U.S.C. § 21081(a) (setting out minimum standards for voting systems used
7 in federal elections). HAVA further requires the EAC to adopt a set of Voluntary
8 Voting System Guidelines, including requirements for accuracy, reliability, and
9 security, and to provide for the testing and certification of voting systems (*i.e.*, federal
10 certification). Arizona law provides Arizona-specific requirements for a voting system
11 to be used in Arizona elections, which includes meeting the requirements of HAVA,
12 being tested by a federal voting system testing laboratory (“VSTL”), and certified by the
13 Secretary of State’s Office.

14 9. Section 4.2 of the Arizona Senate/Cyber Ninjas Statement of Work
15 (SOW), entitled *Vote and Tally Phases*, describes “Scanning of ballots” as in scope, yet
16 defines no methodology for this process. The equipment set up on the tables for the
17 recount, as I observed inside the Arizona Veterans Memorial Coliseum on Thursday,
18 April 22, 2021 and through the live video feed was not equipment that the EAC has
19 certified nor has any federally accredited VSTLs tested for accuracy, reliability, and
20 security.

21 10. While no detailed counting procedures have been made public, based on
22 what I observed through the live video feed of the audit, and further information
23 provided at the April 22, 2021 press conference, the process for the Vote Count & Tally
24 Phase, appears to involve having one individual take a picture of both sides of the ballot
25

26
27 ³ <https://www.azleg.gov/ars/16/00442.htm>

28 ⁴ https://www.eac.gov/sites/default/files/eac_assets/1/6/HAVA41.PDF

1 using the uncertified, untested scanning hardware and software supplied by Cyber
2 Ninjas.

3 11. The picture of the ballot is then brought up on three screens, with a
4 counter (person) sitting in front of each screen. The counter is supposed to review the
5 paper ballot to ensure it is the same as the ballot on screen and then tally the vote off of
6 the image on screen.

7 12. While the original paper ballot is placed on a carousel, resembling a “lazy
8 Susan,” which can be spun to each of the three counters to allow them to see the original
9 ballot, in my observation of the live video feed, the counters do not appear to be
10 following the standard process and procedure of verifying the paper ballot to what is on
11 screen because the carousel is being spun too fast to adequately verify that what is
12 displayed on the screen and what is on the original paper ballot are identical. In many
13 instances, the counter is solely spinning the carousel containing the paper ballot without
14 looking at it and tallying solely off the ballot image that was placed on screen via the
15 uncertified, untested scanning hardware and software supplied by Cyber Ninjas.

16 13. The reliance on ballot images created by an untested and uncertified
17 system is particularly puzzling and concerning given that the federally and state tested
18 and certified voting system that Maricopa County used in the November 3, 2020,
19 election created an official ballot image upon the original scan of each ballot.
20 Additionally, the documents produced in response to the January 12, 2021, subpoenas
21 included all electronic images of the ballots cast in Maricopa County in the November
22 3, 2020, general election. Therefore, instead of conducting the on-screen count of
23 ballots using the uncertified, untested hardware and software supplied by Cyber Ninjas,
24 they could and should have used the official electronic ballot images from the federally
25 and state tested and certified voting system that were obtained as part of the subpoena.

26 14. The fact that uncertified and untested equipment is being used to capture
27 and project the ballot image for the Vote & Tally Phase of the audit raises serious
28

1 concerns. For example, this means there has been no testing or certification to ensure
2 that the system used is not preloaded with inaccurate ballot images, or the system’s
3 software is written to manipulate specific images and scanned ballots. Testing and
4 certification by VSTLs and the EAC is designed specifically to protect against such
5 risks, including through a source code review that ensures these risks cannot occur.

6 **II. Opinion 2: The Vote Count & Tally Phase (i.e., hand count) is not a**
7 **hand count that follows industry best practices or Arizona “Hand**
8 **Count Tabulating Methods” that have been developed to ensure**
9 **accuracy, reliability, and security of the count.**

10 15. The methodology of The Vote Count & Tally Phase, as described in
11 Section 5.2 of the SOW refers to the process as a “hand count.” This term has been
12 reiterated in the Press Briefing on Thursday, April 22, 2021, by members of the forensic
13 audit team.

14 16. However, a hand-count is a specific type of counting method and is
15 defined by the U.S. National Institute of Standards and Technology (“NIST”), in its
16 Election Glossary,⁵ as “Counting ballot sheets and/or selections on ballot sheets by
17 human examination.” A ballot is further defined as “Presentation of the contest
18 options for a particular voter.”

19 17. In the case of Maricopa County’s voting system, there are only two types
20 of ballots: (a) a paper ballot that the voter marks, and (b) an electronic ballot – or the
21 interface of a ballot marking device – which creates an output of a paper ballot.

22 18. This is further substantiated in the Arizona Elections Procedures Manual
23 (“EPM”) Section VII, which is entitled “Hand Count Tabulating Methods,” whereby
24 there are only two prescribed methods. The first method is for hand counting paper
25 ballots, whereas the second method is for counting a voter verifiable paper trail
26

27
28

⁵ <https://pages.nist.gov/ElectionGlossary/>

1 (“VVPAT”) – a specific type of paper record that is printed on a direct recording
2 electronic (“DRE”) voting machine, which is not applicable to Maricopa County.

3 19. Based on what I have observed, the counting method being used does not
4 comply with the NIST definition of a hand count or the EPM procedures for hand
5 counting ballots applicable to Maricopa County ballots, both of which would require
6 counting based on the original paper ballot and not a generated image of the ballot, and
7 certainly not an image generated by an untested and uncertified system.

8 **III. Opinion 3: The review of non-voting system technologies under the**
9 **“Electronic Voting System Phase” could lead to inaccurate and**
10 **invalid electronic voting system test results and findings.**

11 20. One of the four phases of The Arizona Senate Cyber Ninjas Statement of
12 Work (SOW) for the forensic audit is the “Electronic Voting Systems Phase.” This
13 phase involves two technologies that are not “electronic voting systems.”

14 21. HAVA defines an electronic voting system i as the total combination of
15 mechanical, electromechanical, or electronic equipment (including the software,
16 firmware, and documentation required to program, control, and support the equipment)
17 that is used— (A) to define ballots; (B) to cast and count votes; (C) to report or display
18 election results; and (D) to maintain and produce any audit trail information. 52 U.S.C.
19 § 21081(b). This definition is replicated in Chapter 4 of the Arizona 2019 EPM.⁶
20 Additionally, the EPM states “Thus, a voting system consists of the electronic voting
21 equipment (including central count equipment, precinct voting equipment, and
22 accessible voting equipment) and election management system (EMS) used to tabulate
23 ballots.”

24 22. The SOW, in Section 4.3, includes review of Maricopa County’s
25 SiteBook, an electronic poll book – a non-voting system technology – as being included
26

27 ⁶
28 https://azsos.gov/sites/default/files/2019_ELECTIONS_PROCEDURES_MANUAL_APPROVED.pdf (Page 90)

1 within the scope. This technology is used to validate the registration and authenticate
2 the voter, in order for her/him to begin the voting process - a precursor to the act of
3 voting. SiteBook does not meet the definition of voting equipment and is not part of the
4 electronic voting system and therefore are not subject to the same standards under
5 federal guidelines or state law.

6 23. The SOW Section 6.3 includes SiteBook as well as the NOVUS system.
7 The NOVUS system is a Runbeck Election Services ballot duplication component and
8 is not part of the electronic voting system nor is it listed as a component within the
9 scope of the Electronic Voting Phase, as defined in Section 4 of the SOW entitled
10 “Scope & Service Description.” Therefore, the NOVUS system is also not subject to the
11 same standards as components of the electronic voting system under federal guidelines
12 or state law.

13 24. The Statement of Work’s apparent conflation of the SiteBook and
14 NOVUS systems as part of the electronic voting system indicates a lack of
15 understanding for technical specifications and standards that apply to various aspects of
16 election technology, and risks reaching conclusions that mislead the public regarding
17 whether equipment used in Maricopa County in the 2020 election meet the standards
18 and requirements that apply to the particular type of equipment.

19 25.

20 **IV. Opinion 4: The physical security does not meet best practices for**
21 **protecting election infrastructure.**

22 26. On January 6, 2017, then Secretary of Homeland Security Jeh Johnson,
23 designated elections infrastructure as critical infrastructure⁷ meaning that “assets,
24 systems, and networks, whether physical or virtual, are considered so vital to the United
25 States that their incapacitation or destruction would have a debilitating effect on
26

27

⁷ [https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-
infrastructure-critical](https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-
28 infrastructure-critical)

1 security, national economic security, national public health or safety, or any
2 combination thereof.”⁸

3 27. The U.S. Department of Homeland Security (DHS) Cybersecurity and
4 Infrastructure Security Agency (CISA) released published *Election Security – Physical*
5 *Security of Voting Locations and Election Facilities*,⁹ which outlines mitigative
6 measures and compensating controls for physically securing locations that house
7 election infrastructure (i.e., storage facilities, polling places, and centralized vote
8 tabulation locations). A best practice listed in the document is to “Evaluate your security
9 requirements and design an inspection program to enhance the capacity to monitor,
10 report, and respond to incidents occurring in and around all election infrastructure,
11 election facilities, and voting locations.

12 28. Section III, subsection A of the EPM is entitled Physical Security of the
13 Electronic Voting System, states “Must be stored in a locked, secured location that
14 prevents unauthorized access.”

15 29. I observed that official ballots are in boxes that are secured inside locked
16 cages – yet it does not have a ceiling, so people could climb over – inside the Arizona
17 Veterans Memorial Coliseum. However, the equipment being used in “Vote Count &
18 Tally” Phase is sitting in an unsecured, open area of the Arizona Veterans Memorial
19 Coliseum, as visible in the live video feed of the audit.

20 30. What I observed is consistent with the concerns raised by multiple media
21 reporters, including with video recordings, of the Arizona Veterans Memorial Coliseum
22 being inadequately secured and non-credentialed individuals being able to enter the
23 facility.

24
25
26
27 ⁸ <https://www.cisa.gov/critical-infrastructure-sectors>

28 ⁹ https://www.cisa.gov/sites/default/files/publications/physical-security-of-voting-location-election-facilities_v2_508.pdf

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

31. On April 22, 2021, when I arrived at the Arizona Veterans Memorial Coliseum, there were no signs in the parking lot describing where the media and public needed to go to receive credentials. The security personnel waved my Lyft driver to the area where all the media was parked. I got out of the car and followed a cameraman up the stairs to the concourse level, where a door was propped open with a doorstop and left unattended. I proceeded to the seats where I sat and awaited the press briefing, but I did not see any protective measures that would have prohibited me from walking around with unfettered access.

32. During the April 22, 2021, press release, a door was left open and members of the press, as well as member(s) of the public were able to enter the building without receiving credentials.

33. Based on what I observed in-person at the Arizona Veterans Memorial Coliseum and through the live video feed, and from additional media reports, the security procedures being employed do not comport with the requirements in the EPM or CISA’s guidelines for securing election infrastructure. The security procedures in room I was in, where the tally process was being conducted, is not in accordance with the requirements in the EPM or CISA guidelines for physical security, and ballots and voting equipment stored under such conditions would not be adequately secured pursuant to the EPM or CISA guidelines.

DATED this 25th day of April, 2021.

By /s/ Ryan Macias
Ryan Macias

Exhibit 1

Ryan Macias

RSM Election Solutions LLC



Professional Profile

Advising, strategizing, and developing policy for 15 years with a proven record of significant, successful contributions in election administration, election infrastructure, technology security, and standards development.

Experience

RSM Election Solutions LLC– Election Technology & Cybersecurity Consultant/Owner: (05/2019 – Present)

Develop methodologies and strategies for evaluating critical products, assets, and appliances used to secure critical infrastructure, with emphasis on election infrastructure technologies.

Assess the needs of United States (U.S.) and International government entities, particularly election authorities, in procuring and implementing cybersecurity infrastructure projects.

Provide expert research, analyses, and recommendations on U.S. funding of international government entities, such as U.S. Agency for International Development (USAID) funded projects for securing democratic institutions around the world.

Audit the resiliency and cybersecurity of major critical infrastructure projects to identify risk, estimate the impact, and assess the value added.

Advise election officials on process, procedures, rules, and regulations to address changes in election technology infrastructure and election administration.

Testify, provide oral testimony, written declarations, and consultation on election technology and security litigations and hearings in state and federal courts.

Lafayette Group Inc.– Subject Matter Expert, Election Security: (05/2019 – Present)

Strategize, advise, and provide stakeholder engagement to the Election Security Initiative (ESI) at Cybersecurity and Infrastructure Security Agency (CISA).

Partner with state and local election officials to build resiliency in their election infrastructure by assessing risk and identifying resources that can mitigate the risk.

Collaborating with election officials, election infrastructure providers, non-governmental organizations, and the electorate on the risks to the democratic process.

U.S. EAC– Acting Director, Testing & Certification (03/2019 – 05/2019)

Managed the development of publications and trainings for stakeholders on election technology and cybersecurity.

Served as the U.S. Election Assistance Commission (EAC) lead on critical infrastructure issues.

Lead to the [Technical Guidelines Development Committee](#) (TGDC) a federal advisory committee encompassing experts in the field of security, accessibility, standards development that advise on the development of HAVA compliant election technology principles, guidelines, and standards.

Collaborated with state and local election officials implementing new legislation, rules, regulations, and standards for election infrastructure.

Developed strategies and methodologies for balancing security with accessibility in election technology in compliance with the Help America Vote Act (HAVA) 2002.

U.S. EAC– Sr. Election Technology Program Specialist (05/2016 – 05/2019)

Engineered a new strategic approach for federal certification of voting systems, restructuring internal policies, processes, and procedures - focusing on the auditing and conformance to International standards for security, quality assurance, and configuration management.

Transformed the scope of voting system standards to implement a functional process-based model providing adaptability across multiple election technologies.

Project Manager for federal voting system certification - analyzing voting systems to determine conformance with federal standards, policies, and procedures.

Developed nationally recognized publications and trainings on the best practices for securing, procuring, and implementing election technology; many of which have been referenced in technical or policy related publications.

Implemented a risk-based approach to analyze and identify current threats and challenges in election technology, particularly regarding cybersecurity and information operations.

California Secretary of State– Sr. Election Technology Analyst (08/2006 – 05/2016)

Collaborated with legislators, election officials, and special interest groups to develop legislation, regulations, and policies for election systems including the [California Voters Choice Act](#), [California Voting System Standards](#), and [remote accessible vote by mail systems](#) legislation and standards.

Advise the Secretary of State and Executive Staff on the certification and implementation of election technologies, such as voting systems and remote accessible vote by mail technologies to ensure that all voters have an opportunity to vote privately and independently.

Education & Professional Certifications

Bachelor of Science, Business Administration (Finance) – California State University, Sacramento

Certified Election/Registration Administrator (CERA)

Lead Auditor - ISO 9001 & ISO 17025

Certified as a Protected Critical Infrastructure Information (PCII) Authorized User

Organizations & Committees

Member – [National Task Force on Election Crises](#)

Program Committee Member – [E-Vote-ID 2020](#): International Conference for Electronic Voting

Steering Committee Member for the Center for Internet Security (CIS) [Rapid Architecture-Based Election Technology Verification \(RABET-V\)](#)

Former State of California appointee to the [U.S. EAC's Standards Board](#)

Projects & Publications

- [Rebuttal Report](#) to the Allied Security Operation Group (ASOG) Antrim Michigan Forensics Report.
- [Election Security Risk in Focus: Ransomware](#) – Trained hundreds of election administrators on the cybersecurity risks and mitigative measures related to ransomware in the election infrastructure.
- [MEMORANDUM in Opposition re13 MOTION for Preliminary Injunction](#): Harley et al v. Kosinski et al, United States District Court in the Eastern District of New York, Case #1:20-cv-04664.
- [MEMORANDUM in Opposition re26 MOTION for Preliminary Injunction](#): Taliaferro et al v. North Carolina State Board of Elections et al, United States District Court for the Eastern District of North Carolina Western Division, Case #5:20-cv-00411.
- [Election Security Risk Profile Tool](#) – Collaborator on the methodology for a simple, non-technical tool that provides mitigations for the non-cybersecurity professionals to understand.
- Co-Author of the Harvard Belfer Center Defending Digital Democracy Project (D3P) [State and Local Election Cybersecurity Playbook](#) and [The Elections Battle Staff Playbook](#).
- Trainer and scenario builder for the D3P [State and Local Election Official Tabletop Exercise](#) and [Battle Staff Bootcamp](#).
- Contributor to CIS [A Handbook Election Infrastructure Security](#) and [Election Technology Procurement Guide](#).
- Lead on [EAC Voluntary Voting System Guidelines v. 2.0](#) focusing on providing technologies that are both secure and accessible.
- Created the 17-Functions process model that defined the [Scope of the VVSG 2.0](#) so that non-traditional election technologies could be tested to the same standards as traditional voting systems.

Exhibit 2

Cyber Ninjas, Inc. Master Services Agreement

This Master Services Agreement (the “Master Agreement”) is entered into as of the 31 day of March, 2021 (the “Effective Date”), between Cyber Ninjas, Inc., a Florida Corporation, (the “Contractor”), and the Arizona State Senate (the “Client”). Contractor and Client are referred to herein individually as a “Party” and collectively as the “Parties”.

WHEREAS, Client desires to retain Contractor, and Contractor desires to provide to Client the consulting and/or professional services described herein; and

WHEREAS, Client and Contractor desire to establish the terms and conditions that will regulate all relationships between Client and Contractor.

NOW THEREFORE, in consideration of the mutual covenants and promises contained herein and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties hereby agree as follows:

1 SCOPE OF AGREEMENT

This Master Agreement establishes a contractual framework for Contractor’s consulting and/or professional services as described herein. The Parties agree to the terms and conditions set forth in this Master Agreement and in any Statement of Work executed by the Parties referencing this Master Agreement. Each Statement of Work is incorporated into this Master Agreement, and the applicable portions of this Master Agreement are incorporated into each Statement of Work. The Statement(s) of Work and this Master Agreement are herein collectively referred to as the “Agreement.”

2 STRUCTURE OF AGREEMENT.

- 2.1 Components of the Agreement. The Agreement consists of:
- (a) The provisions set forth in this Master Agreement and the Exhibits referenced herein;
 - (b) The Statement(s) of Work attached hereto, and any Schedules referenced therein; and
 - (c) Any additional Statements of Work executed by the Parties pursuant to this Agreement, including the Schedules referenced in each such Statement of Work.
- 2.2 Statement(s) of Work. The Services (as defined in Article 4) that Contractor will provide for Client will be described in and be the subject of (i) one or more Statements of Work executed by the Parties pursuant to this Agreement, and (ii) this Agreement. Each Statement of Work shall be substantially in the form of, and shall include the set of Schedules described in, “Exhibit 1-Form of Statement of Work”, with such additions, deletions and modifications as the Parties may agree.
- 2.3 Deviations from Agreement, Priority. In the event of a conflict, the terms of the Statements of Work shall be governed by the terms of this Master Agreement, unless an applicable Statement of Work expressly and specifically notes the deviations from the terms of this Master Agreement for the purposes of such Statement of Work.

3 TERM AND TERMINATION.

- 3.1 Term of Master Agreement. The Term of the Master Agreement will begin as of the Effective Date and shall continue until terminated as provided in Section 3.3 (the "Term").
- 3.2 Term of Statements of Work. Each Statement of Work will have its own term and will continue for the period identified therein unless terminated earlier in accordance with Section 3.4 (the "Service Term"). In the event that the Service Term on any applicable Statement of Work expires and Services continue to be provided by Contractor and received and used by Client, the terms and conditions of the Master Agreement shall apply until the Services have been terminated.
- 3.3 Termination of Master Agreement. Either Party may terminate this Agreement immediately upon written notice to the other Party if there is no Statement of Work in effect.
- 3.4 Termination of Statement of Work by Client. A Statement of Work may be terminated by Client, for any reason other than Contractor's breach, upon fourteen (14) days prior written notice to Contractor. In such event, (i) Contractor shall cease its activities under the terminated Statement of Work on the effective date of termination; and (ii) Client agrees to pay to Contractor all amounts for any amounts due for Services performed through the effective termination date. (iii) In the case of fixed price work whereby the effective date of termination is after Contractor has or will commence the Services, Client agrees to pay Contractor an amount that will be determined on a pro-rata basis computed by dividing the total fee for the Service by the number of days required for completion of the Services and multiplying the result by the number of working days completed at the effective date of termination. (iv) Client agrees to pay to Contractor all costs in full associated with equipment or other non-Service related costs that were incurred before the effective termination date.
- 3.5 Termination for Breach. Either party may terminate the Agreement in the event that the other party materially defaults in performing any obligation under this Agreement (including any Statement of Work) and such default continues un-remedied for a period of seven (7) days following written notice of default. If Client terminates the Agreement and/or any Statement of Work as a result of Contractor's breach, then to the extent that Client has prepaid any fees for Services, Contractor shall refund to Client any prepaid fees on a pro-rata basis to the extent such fees are attributable to the period after such termination date.
- 3.6 Effect of Termination. Upon termination or expiration of this Agreement and/or a Statement of Work: (i) the parties will work together to establish an orderly phase-out of the Services; (ii) Client will pay Contractor for any amounts due under the Agreement, including all Services rendered under the terminated Statement of Work up to the effective date of the termination; and (iii) each Party will promptly cease all use of and destroy or return, as directed by the other Party, all Confidential Information of the other Party except for all audit records (including but not limited to work papers, videotapes, images, tally sheets, draft reports and other documents generated during the audit) which will be held in escrow in a safe approved by the GSA for TS/SCI material for a period of three years and available to the Contractor and Client solely for purposes of addressing any claims, actions or allegations regarding the audit (the "Escrow"), provided that, pursuant to Section 15.4, the Parties shall provide to each other documents and information that are reasonably necessary to the defense of any third party claims arising out of or related to the subject matter of this Agreement.

4 SERVICES.

- 4.1 Definitions.
- 4.1.1 “Services” shall mean consulting, training or any other professional services to be provided by Contractor to Client, as more particularly described in a Statement of Work, including any Work Product provided in connection therewith.
- 4.1.2 “Work Product” shall mean any deliverables which are created, developed or provided by Contractor in connection with the Services pursuant to a Statement of Work, excluding any Contractor’s Intellectual Property.
- 4.1.3 “Contractor’s Intellectual Property” shall mean all right, title and interest in and to the Services, including, but not limited to, all inventions, skills, know-how, expertise, ideas, methods, processes, notations, documentation, strategies, policies, reports (with the exception of the data within the reports, as such data is the Client’s proprietary data) and computer programs including any source code or object code, (and any enhancements and modifications made thereto), developed by Contractor in connection with the performance of the Services hereunder and of general applicability across Contractor’s customer base. For the avoidance of doubt, the term shall not include (1) the reports prepared by Contractor for Client (other than any standard text used by Contractor in such reports) pursuant to this Agreement or any Statement of Work, which shall be the exclusive property of Client and shall be considered “works made for hire” within the meaning of the Copyright Act of 1976, as amended; and (2) any data or process discovered on or obtained from the Dominion devices that will be the subject of the forensic review.
- 4.2 Obligation to Provide Services. Starting on the Commencement Date of each Statement of Work and continuing during each Statement of Work Term, Contractor shall provide the Services described in each such Statement of Work to, and perform the Services for, Client in accordance with the applicable Statement of Work and the Agreement.
- 4.3 Contractor’s Performance. Contractor will perform the Services set forth in each Statement of Work using personnel that have the necessary knowledge, training, skills, experience, qualifications and resources to provide and perform the Services in accordance with the Agreement. Contractor shall render such Services in a prompt, professional, diligent, and workmanlike manner, consistent with industry standards applicable to the performance of such Services.
- 4.4 Client’s Obligations. Client acknowledges that Contractor’s performance and delivery of the Services are contingent upon: (i) Client providing full access to such information as may be reasonably necessary for Contractor to complete the Services as described in the Statement(s) of Work including access to its personnel, facilities, equipment, hardware, network and information, as applicable; and (ii) Client promptly obtaining and providing to Contractor any required licenses, approvals or consents necessary for Contractor’s performance of the Services. Contractor will be excused from its failure to perform its obligations under this Agreement to the extent such failure is caused by Client’s delay in performing or failure to perform its responsibilities under this Agreement and/or any Statement of Work.
- 4.5 Location of Services. Contractor shall provide the Services at the site designated in the applicable Statement of Work.

- 4.6 Status Reports. Contractor shall keep Client informed of the status of the Services and provide Client with such status reports and other reports and information regarding the Services as reasonably requested by Client.
- 4.7 New Services. During the Term, Client may request that Contractor provide New Services for Client. New Services may be activities that are performed on a continuous basis for the remainder of the Term or activities that are performed on a project basis. Any agreement of the Parties with respect to New Services will be in writing and shall also become a "Service" and be reflected in an additional Statement of Work hereto or in an amendment to an existing Statement of Work hereunder.
- 4.8 Change of Services. "Change of Services" means any change to the Services as set forth in the Statement of Work that (i) would modify or alter the delivery of the Services or the composition of the Services, (ii) would alter the cost to Client for the Services, or (iii) is agreed by Client and Contractor in writing to be a Change. From time to time during the Term, Client or Contractor may propose Changes to the Services.
- The following process is required to effectuate a Change of Services by either Party:
- 4.9 A Project Change Request ("PCR") will be the vehicle for communicating change. The PCR must describe the change, the rationale for the change, and the effect the change will have on the Services.
- 4.10 The designated project manager of the requesting Party will review any proposed change prior to submitting the PCR to the other Party.
- 4.11 Contractor and Client will mutually agree upon any additional fees for such investigation, if any. If the investigation is authorized, the Client project manager will sign the PCR, which will constitute approval for the investigation charges. Contractor will invoice Client for any such charges. The investigation will determine the effect that the implementation of the PCR will have on Statement of Work terms and conditions.
- 4.12 Upon completion of the investigation, both parties will review the impact of the proposed change and, if mutually agreed, a written addendum to the Statement of Work must be signed by both Parties to authorize implementation of the investigated changes that specifically identifies the portion of the Statement of Work that is the subject of the modification or amendment and the changed or new provision(s) to the Statement of Work.
- 4.13 End Client Requirements. If Contractor is providing Services for Client that is intended to be for the benefit of a customer of Client ("End Client"), the End Client should be identified in an applicable Statement of Work. The Parties shall mutually agree upon any additional terms related to such End Client which terms shall be set forth in a Schedule to the applicable Statement of Work.
- 4.14 Client Reports; No Reliance by Third Parties. Contractor will provide those reports identified in the applicable Statement of Work ("Client Report"). The Client Report is prepared uniquely and exclusively for Client's sole use. The provision by Client of any Client Report or any information therein to any third party shall not entitle such third party to rely on the Client Report or the contents thereof in any manner or for any purpose whatsoever, and Contractor specifically disclaims all liability for any damages whatsoever (whether foreseen or unforeseen, direct, indirect, consequential, incidental, special, exemplary or punitive) to such third party arising from or related to reliance by such third party on any Client Report or any contents thereof.

- 4.15 Acceptance Testing. Unless otherwise specified in an Statement of Work, Client shall have a period of fourteen (14) days to perform Acceptance Testing on each deliverable provided by Contractor to determine whether it conforms to the Specifications and any other Acceptance criteria (collectively as the "Acceptance Criteria") stated in the Statement of Work. If Client rejects the deliverable as non-conforming, unless otherwise agreed to by the parties, Contractor shall, at its expense, within fourteen (14) days from the date of notice of rejection, correct the deliverable to cause it to conform to the Acceptance Criteria and resubmit the deliverable for further Acceptance testing in accordance with the process specified in this Section 4.15. In the event that the deliverable does not conform to the Acceptance Criteria after being resubmitted a second time, Client, may at its option, (i) provide Contractor with another fourteen (14) days to correct and resubmit the deliverable or (ii) immediately terminate the Statement of Work and obtain a refund of any amounts paid for the non-conforming Services pursuant to the applicable Statement of Work.

5 FEES AND PAYMENT TERMS.

- 5.1 Fees. Client agrees to pay to Contractor the fees for the Services in the amount as specified in the applicable Statement of Work.
- 5.2 Invoices. Contractor shall render, by means of an electronic file, an invoice or invoices in a form containing reasonable detail of the fees incurred in each month. Upon completion of the Services as provided in the Statement of Work, Contractor shall provide a final invoice to Client. Contractor shall identify all taxes and material costs incurred for the month in each such invoice. All invoices shall be stated in US dollars, unless otherwise specified in the Statement of Work.
- 5.3 Payment Terms. All invoices are due upon receipt. Payment not received within 30 days of the date of the invoice is past due. Contractor reserves the right to suspend any existing or future Services when invoice becomes thirty (30) days past due. Client shall pay 1.5% per month non-prorated interest on any outstanding balances in excess of thirty days past due. If it becomes necessary to collect past due payments, Client shall be responsible for reasonable attorney fees required in order to collect upon the past-due invoice(s).
- 5.4 Taxes. The applicable Statement of Work shall prescribe the parties' respective responsibilities with respect to the invoicing and payment of state sales, use, gross receipts, or similar taxes, if any, applicable to the Services and deliverables to be provided by Contractor to Client. Client shall have no responsibility with respect to federal, state, or local laws arising out of Contractor's performance of any Statement of Work, including any interest or penalties.

6 PERSONNEL.

- 6.1 Designated Personnel. Contractor shall assign employees that are critical to the provision and delivery of the Services provided (referred to herein as "Designated Personnel") and except as provided in this Article 6, shall not be removed or replaced at any time during the performance of Services in a Statement of Work, except with Client's prior written consent.
- 6.2 Replacement of Designated Personnel by Contractor. Notwithstanding the foregoing, if any Designated Personnel becomes unavailable for reasons beyond Contractor's reasonable control or Designated Personnel's professional relationship with Contractor terminates for any reason,

Contractor may replace the Designated Personnel with a similarly experienced and skilled employee. In such event, Contractor shall provide immediate notification to Client of a change in a Designated Personnel's status.

- 6.3 Replacement of Designated Personnel by Client. In the event that Client is dissatisfied for any reason with any Designated Personnel, Client may request that Contractor replace the Designated Personnel by providing written notice to Contractor. Contractor shall ensure that all Designated Personnel are bound by the terms and conditions of this Agreement applicable to their performance of the Services and shall be responsible for their compliance therewith.
- 6.4 Background Screening. Contractor shall have performed the background screening described in Exhibit 2 (Background Screening Measures) on all of its agents and personnel who will have access to Client Confidential Information prior to assigning such individuals or entities to provide Services under this Agreement.

7 PROPRIETARY RIGHTS.

- 7.1 Client's Proprietary Rights. Client represents and warrants that it has the necessary rights, power and authority to transmit Client Data (as defined below) to Contractor under this Agreement and that Client has and shall continue to fulfil all obligations with respect to individuals as required to permit Contractor to carry out the terms hereof, including with respect to all applicable laws, regulations and other constraints applicable to Client Data. As between Client and Contractor, Client or a political subdivision or government entity in the State of Arizona owns all right, title and interest in and to (i) any data provided by Client (and/or the End Client, if applicable) to Contractor; (ii) any of Client's (and/or the End Client, if applicable) data accessed or used by Contractor or transmitted by Client to Contractor in connection with Contractor's provision of the Services (Client's data and Client's End User's data, collectively, the "Client Data"); (iii) all intellectual property of Client ("Client's Intellectual Property") that may be made available to Contractor in the course of providing Services under this Agreement.
- 7.2 License to Contractor. This Agreement does not transfer or convey to Contractor any right, title or interest in or to the Client Data or any associated Client's Intellectual Property. Client grants to Contractor a limited, non-exclusive, worldwide, revocable license to use and otherwise process the Client Data and any associated Client's Intellectual Property to perform the Services during the Term hereof. Contractor's permitted license to use the Client Data and Client's Intellectual Property is subject to the confidentiality obligations and requirements for as long as Contractor has possession of such Client Data and Intellectual Property.

7.3 Contractor's Proprietary Rights. As between Client and Contractor, Contractor owns all right, title and interest in and to the Services, including, Contractor's Intellectual Property. Except to the extent specifically provided in the applicable Statement of Work, this Agreement does not transfer or convey to Client or any third party any right, title or interest in or to the Services or any associated Contractor's Intellectual Property rights, but only grants to Client a limited, non-exclusive right and license to use as granted in accordance with the Agreement. Contractor shall retain all proprietary rights to Contractor's Intellectual Property and Client will take no actions which adversely affect Contractor's Intellectual Property rights. **For the avoidance of doubt and notwithstanding any other provision in this Section or elsewhere in the Agreement, all documents, information, materials, devices, media, and data relating to or arising out of the administration of the November 3, 2020 general election in Arizona, including but not limited to voted ballots, images of voted ballots, and any other materials prepared by, provided by, or originating from the Client or any political subdivision or governmental entity in the State of Arizona, are the sole and exclusive property of the Client or of the applicable political subdivision or governmental entity, and Contractor shall have no right or interest whatsoever in such documents, information, materials, or data.**

8 NONDISCLOSURE.

8.1 Confidential Information. "Confidential Information" refers to any information one party to the Agreement discloses (the "Disclosing Party") to the other (the "Receiving Party"). The confidential, proprietary or trade secret information in the context of the Agreement may include, but is not limited to, business information and concepts, marketing information and concepts, financial statements and other financial information, customer information and records, corporate information and records, sales and operational information and records, and certain other information, papers, documents, studies and/or other materials, technical information, and certain other information, papers, documents, digital files, studies, compilations, forecasts, strategic and marketing plans, budgets, specifications, research information, software, source code, discoveries, ideas, know-how, designs, drawings, flow charts, data, computer programs, market data; digital information, digital media, and any and all electronic data, information, and processes stored on Maricopa County servers, portable storage media and/or cloud storage (remote servers) technologies, and/or other materials, both written and oral. Notwithstanding the foregoing, Confidential Information does not include information that: (i) is in the Receiving Party's possession at the time of disclosure; (ii) is independently developed by the Receiving Party without use of or reference to Confidential Information; (iii) becomes known publicly, before or after disclosure, other than as a result of the Receiving Party's improper action or inaction; or (iv) is approved for release in writing by the Disclosing Party.

- 8.2 Nondisclosure Obligations. The Receiving Party will not use Confidential Information for any purpose other than to facilitate performance of Services pursuant to the Agreement and any applicable Statement of Work. The Receiving Party: (i) will not disclose Confidential Information to any employee or contractor or other agent of the Receiving Party unless such person needs access in order to facilitate the Services and executes a nondisclosure agreement with the Receiving Party, substantially in the form provided in Exhibit 3; and (ii) will not disclose Confidential Information to any other third party without the Disclosing Party's prior written consent. Without limiting the generality of the foregoing, the Receiving Party will protect Confidential Information with the same degree of care it uses to protect its own Confidential Information of similar nature and importance, but with no less than reasonable care. The Receiving Party will promptly notify the Disclosing Party of any misuse or misappropriation of Confidential Information that comes to the Receiving Party's attention. Notwithstanding the foregoing, the Receiving Party may disclose Confidential Information as required by applicable law or by proper legal or governmental authority; however, the Receiving Party will give the Disclosing Party prompt notice of any such legal or governmental demand and will reasonably cooperate with the Disclosing Party in any effort to seek a protective order or otherwise to contest such required disclosure, at the Disclosing Party's expense. For the avoidance of doubt, this provision prohibits the Contractor and its agents from providing data, information, reports, or drafts to anyone without the prior written approval of the Client. The Client will determine in its sole and unlimited discretion whether to grant such approval.
- 8.3 Injunction. The Receiving Party agrees that breach of this Article 8 might cause the Disclosing Party irreparable injury, for which monetary damages would not provide adequate compensation, and that in addition to any other remedy, the Disclosing Party will be entitled to injunctive relief against such breach or threatened breach, without proving actual damage or posting a bond or other security.
- 8.4 Return. Upon the Disclosing Party's written request and after the termination of the Escrow, the Receiving Party will return all copies of Confidential Information to the Disclosing Party or upon authorization of Disclosing Party, certify in writing the destruction thereof.
- 8.5 Third Party Hack. Contractor shall not be liable for any breach of this Section 8 resulting from a hack or intrusion by a third party into Client's network or information technology systems unless the hack or intrusion was through endpoints or devices monitored by Contractor and was caused directly by Contractor's gross negligence or wilful misconduct. For avoidance of doubt, Contractor shall not be liable for any breach of this Section 8 resulting from a third-party hack or intrusion into any part of Client's network, or any environment, software, hardware or operational technology, that Contractor is not obligated to monitor pursuant to a Statement of Work executed under this Agreement.
- 8.6 Retained Custody of Ballots. The Client shall retain continuous and uninterrupted custody of the ballots being tallied. For the avoidance of doubt, this provision requires Contractor and each of its agents to leave all ballots at the counting facility at the conclusion of every shift.

8.7 Survival. This Section 8 shall survive for three (3) years following any termination or expiration of this Agreement; provided that with respect to any Confidential Information remaining in the Receiving Party's possession following any termination or expiration of this Agreement, the obligations under this Section 8 shall survive for as long as such Confidential Information remains in such party's possession.

9 NO SOLICITATION.

Contractor and Client agree that neither party will, at any time within twelve (24) months after the termination of the Agreement, solicit, attempt to solicit or employ any of the personnel who were employed or otherwise engaged by the other party at any time during which the Agreement was in effect, except with the express written permission of the other party. The Parties agree that the damages for any breach of this Article 9 will be substantial, but difficult to ascertain. Accordingly, the party that breaches this Article 9, shall pay to other party an amount equal to two times (2x) the annual compensation of the employee solicited or hired, which amount shall be paid as liquidated damages, as a good faith effort to estimate the fair, reasonable and actual damages to the aggrieved party and not as a penalty. Nothing in the Agreement shall be construed to prohibit either party from pursuing any other available rights or remedies it may have against the respective employee(s).

10 DATA PROTECTION

10.1 Applicability. This Article 10 shall apply when Contractor is providing Services to Client which involves the processing of Personal Data which is subject to Privacy Laws.

10.2 Definitions. For purposes of this Article 10:

- (a) "Personal Data" means any information relating to an identified or identifiable natural person which is processed by Contractor, acting as a processor on behalf of the Client, in connection with the provision of the Services and which is subject to Privacy Laws.
- (b) "Privacy Laws" means any United States and/or European Union data protection and/or privacy related laws, statutes, directives, judicial orders, or regulations (and any amendments or successors thereto) to which a party to the Agreement is subject and which are applicable to the Services.

10.3 Contractor's Obligations. Contractor will maintain industry-standard administrative, physical, and technical safeguards for protection of the security, confidentiality, and integrity of Personal Data. Contractor shall process Personal Data only in accordance with Client's reasonable and lawful instructions (unless otherwise required to do so by applicable law). Client hereby instructs Contractor to process any Personal Data to provide the Services and comply with Contractor's rights and obligations under the Agreement and any applicable Statement of Work. The Agreement and any applicable Statement of Work comprise Client's complete instructions to Contractor regarding the processing of Personal Data. Any additional or alternate instructions must be agreed between the parties in writing, including the costs (if any) associated with complying with such instructions. Contractor is not responsible for determining if Client's instructions are compliant with applicable law, however, if Contractor is of the opinion that a Client instruction infringes applicable Privacy Laws, Contractor shall notify Client as soon as reasonably practicable and shall not be required to comply with such infringing instruction.

- 10.4 Disclosures. Contractor may only disclose the Personal Data to third parties for the purpose of: (i) complying with Client's reasonable and lawful instructions; (ii) as required in connection with the Services and as permitted by the Agreement and any applicable Statement of Work; and/or (iii) as required to comply with Privacy Laws, or an order of any court, tribunal, regulator or government agency with competent jurisdiction to which Contractor is subject, provided that Contractor will (to the extent permitted by law) inform the Client in advance of any disclosure of Personal Data and will reasonably co-operate with Client to limit the scope of such disclosure to what is legally required.
- 10.5 Demonstrating Compliance. Contractor shall, upon reasonable prior written request from Client (such request not to be made more frequently than once in any twelve-month period), provide to Client such information as may be reasonably necessary to demonstrate Contractor's compliance with its obligations under this Agreement.
- 10.6 Liability and Costs. Contractor shall not be liable for any claim brought by Client or any third party arising from any action or omission by Contractor or Contractor's agents to the extent such action or omission was directed by Client or expressly and affirmatively approved or ratified by Client.

11 DATA RETENTION

- 11.1 Client's Intellectual Property and Confidential Information. All Client Intellectual Property and Client Confidential Information (to include Client Intellectual Property or Client Confidential Information that is contained or embedded within other documents, files, materials, data, or media) shall be removed from all Contractor controlled systems as soon as it is no longer required to perform Services under this Agreement and held in the Escrow. In addition, pursuant to Section 15.4, the Parties shall provide to each other documents and information that are reasonably necessary to the defense of any third party's claims arising out of or related to the subject matter of this Agreement.

12 REPRESENTATIONS AND WARRANTIES.

- 12.1 Representations and Warranties of Client. Client represents and warrants to Contractor as follows:
- (a) Organization; Power. As of the Effective Date, Client (i) is a government entity in the State of Arizona, duly organized, validly existing and in good standing under the Laws of the State of Arizona, and (ii) has full corporate power to conduct its business as currently conducted and to enter into the Agreement.
 - (b) Authorized Agreement. This Agreement has been, and each Statement of Work will be, duly authorized, executed and delivered by Client and constitutes or will constitute, as applicable, a valid and binding agreement of Client, enforceable against Client in accordance with its terms.
 - (c) No Default. Neither the execution and delivery of this Agreement or any Statement of Work by Client, nor the consummation of the transactions contemplated hereby or thereby, shall result in the breach of any term or provision of, or constitute a default under, any charter provision or bylaw, agreement (subject to any applicable consent), order, or law to which Client is a Party or which is otherwise applicable to Client.

12.2 Representations and Warranties of Contractor. Contractor represents and warrants to Client as follows:

- (a) Organization; Power. As of the Effective Date, Contractor (i) is a corporation, duly organized, validly existing and in good standing under the Laws of the State of Florida, and (ii) has full corporate power to own, lease, license and operate its assets and to conduct its business as currently conducted and to enter into the Agreement.
- (b) Authorized Agreement. This Agreement has been, and each Statement of Work will be duly authorized, executed and delivered by Contractor and constitutes or will constitute, as applicable, a valid and binding agreement of Contractor, enforceable against Contractor in accordance with its terms.
- (c) No Default. Neither the execution and delivery of this Agreement or any Statement of Work by Contractor, nor the consummation of the transactions contemplated hereby or thereby, shall result in the breach of any term or provision of, or constitute a default under, any charter provision or bylaw, agreement (subject to any applicable consent), order or law to which Contractor is a Party or that is otherwise applicable to Contractor.

12.3 Additional Warranties of Contractor. Contractor warrants that:

- (a) The Services shall conform to the terms of the Agreement (including the Statement of Work);
- (b) Contractor will comply with all applicable laws, rules and regulations in delivering the Services (including without limitation any privacy, data protection and computer laws);
- (c) The Services shall be performed in a diligent and professional manner consistent with industry best standards;
- (d) Contractor and its agents possess the necessary qualifications, expertise and skills to perform the Services;
- (e) Contractor and all individuals handling Client Confidential Information are either U.S. citizens, or U.S. entities that are owned, controlled, and funded entirely by U.S. citizens.
- (f) Services requiring code review will be sufficiently detailed, comprehensive and sophisticated so as to detect security vulnerabilities in software that should reasonably be discovered given the state of software security at the time the Services are provided;
- (g) Contractor shall ensure that the Services (including any deliverables) do not contain, introduce or cause any program routine, device, or other undisclosed feature, including, without limitation, a time bomb, virus, software lock, drop-dead device, malicious logic, worm, trojan horse, or trap door, that may delete, disable, deactivate, interfere with or otherwise harm software, data, hardware, equipment or systems, or that is intended to provide access to or produce modifications not authorized by Client or any known and exploitable material security vulnerabilities to affect Client's systems (collectively, "Disabling Procedures");

- (h) If, as a result of Contractor's services, a Disabling Procedure is discovered by Contractor, Contractor will promptly notify Client and Contractor shall use commercially reasonable efforts and diligently work to eliminate the effects of the Disabling Procedure at Contractor's expense. Contractor shall not modify or otherwise take corrective action with respect to the Client's systems except at Client's request. In all cases, Contractor shall take immediate action to eliminate and remediate the proliferation of the Disabling Procedure and its effects on the Services, the client's systems, and operating environments. At Client's request, Contractor will report to Client the nature and status of the Disabling Procedure elimination and remediation efforts; and
- (i) Contractor shall correct any breach of the above warranties, at its expense, within fourteen (14) days of its receipt of such notice. In the event that Contractor fails to correct the breach within the specified cure period, in addition to any other rights or remedies that may be available to Client at law or in equity, Contractor shall refund all amounts paid by Client pursuant to the applicable Statement of Work for the affected Services.

13 LIMITATION OF LIABILITY.

IN NO EVENT SHALL CONTRACTOR BE HELD LIABLE FOR INDIRECT, SPECIAL, INCIDENTAL CONSEQUENTIAL, OR PUNITIVE DAMAGES ARISING OUT OF SERVICES PROVIDED HEREUNDER INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUE, BUSINESS INTERRUPTION, LOSS OF USE OF EQUIPMENT, LOSS OF GOODWILL, LOSS OF DATA, LOSS OF BUSINESS OPPORTUNITY, WHETHER CAUSED BY TORT (INCLUDING NEGLIGENCE), COSTS OF SUBSTITUTE EQUIPMENT, OR OTHER COSTS. If applicable law limits the application of the provisions of this Article 13, Contractor's liability will be limited to the least extent permissible.

EXCEPT FOR EACH PARTY'S INDEMNIFICATION OBLIGATIONS UNDER ARTICLE 15 AND NON-SOLICITATION OBLIGATIONS UNDER ARTICLE 9, LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT WILL NOT EXCEED THE TOTAL OF THE AMOUNTS PAID AND PAYABLE TO CONTRACTOR UNDER THE STATEMENT OF WORK(S) TO WHICH THE CLAIM RELATES. THE ABOVE LIMITATIONS WILL APPLY WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY.

14 DISCLAIMER OF WARRANTIES.

EXCEPT AS EXPRESSLY SET FORTH HEREIN, CONTRACTOR MAKES NO EXPRESS OR IMPLIED WARRANTIES WITH RESPECT TO ANY OF THE SERVICES PROVIDED UNDER THIS AGREEMENT, INCLUDING BUT NOT LIMITED TO, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, OR SUITABILITY OR RESULTS TO BE DERIVED FROM THE USE OF ANY SERVICE, SOFTWARE, HARDWARE, DELIVERABLES, WORK PRODUCT OR OTHER MATERIALS PROVIDED UNDER THIS AGREEMENT. CLIENT UNDERSTANDS THAT CONTRACTOR'S SERVICES DO NOT CONSTITUTE ANY GUARANTEE OR ASSURANCE THAT THE SECURITY OF CLIENT'S SYSTEMS, NETWORKS AND ASSETS CANNOT BE BREACHED OR ARE NOT AT RISK. CONTRACTOR MAKES NO WARRANTY THAT EACH AND EVERY VULNERABILITY WILL BE DISCOVERED AS PART OF THE SERVICES AND CONTRACTOR SHALL NOT BE LIABLE TO CLIENT SHOULD VULNERABILITIES LATER BE DISCOVERED.

15 INDEMNIFICATION.

“Indemnified Parties” shall mean, (i) in the case of Contractor, Contractor, and each of Contractor’s respective owners, directors, officers, employees, contractors and agents; and (ii) in the case of Client, Client, and each of Client’s respective members, officers, employees, contractors and agents.

- 15.1 Mutual General Indemnity. Each party agrees to indemnify and hold harmless the other party from (i) any third-party claim or action for personal bodily injuries, including death, or tangible property damage resulting from the indemnifying party’s gross negligence or wilful misconduct; and (ii) breach of this Agreement or the applicable Statement of Work by the indemnifying Party, its respective owners, directors, officers, employees, agents, or contractors.
- 15.2 Contractor Indemnity. Contractor shall defend, indemnify and hold harmless the Client Indemnified Parties from any damages, costs and liabilities, expenses (including reasonable and actual attorney’s fees) (“Damages”) actually incurred or finally adjudicated as to any third-party claim or action alleging that the Services performed or provided by Contractor and delivered pursuant to the Agreement infringe or misappropriate any third party’s patent, copyright, trade secret, or other intellectual property rights enforceable in the country(ies) in which the Services performed or provided by Contractor for Client or third-party claims resulting from Contractor’s gross negligence or wilful misconduct (“Indemnified Claims”). If an Indemnified Claim under this Section 15.2 occurs, or if Contractor determines that an Indemnified Claim is likely to occur, Contractor shall, at its option: (i) obtain a right for Client to continue using such Services; (ii) modify such Services to make them non-infringing; or (iii) replace such Services with a non-infringing equivalent. If (i), (ii) or (iii) above are not reasonably available, either party may, at its option, terminate the Agreement will refund any pre-paid fees on a pro-rata basis for the allegedly infringing Services that have not been performed or provided. Notwithstanding the foregoing, Contractor shall have no obligation under this Section 15.2 for any claim resulting or arising from: (i) modifications made to the Services that were not performed or performed or provided by or on behalf of Contractor; or (ii) the combination, operation or use by Client, or anyone acting on Client’s behalf, of the Services in connection with a third-party product or service (the combination of which causes the infringement).
- 15.3 Client Indemnity. Client shall defend, indemnify and hold harmless the Contractor Indemnified Parties from any Damages actually incurred or finally adjudicated as to any third-party claim, action or allegation: (i) that the Client’s data infringes a copyright or misappropriates any trade secrets enforceable in the country(ies) where the Client’s data is accessed, provided to or received by Contractor or was improperly provided to Contractor in violation of Client’s privacy policies or applicable laws (or regulations promulgated thereunder); (ii) asserting that any action undertaken by Contractor in connection with Contractor’ performance under this Agreement violates law or the rights of a third party under any theory of law, including without limitation claims or allegations related to the analysis of any third party’s systems or processes or to the decryption, analysis of, collection or transfer of data to Contractor; (iii) the use by Client or any of the Client Indemnified Parties of Contractor’s reports and deliverables under this agreement; and (iv) arising from a third party’s reliance on a Client Report, any information therein or any other results or output of the Services. Notwithstanding the foregoing or any other provision of this Agreement, Client shall have (i) no indemnification obligations other than defense costs in connection with any third-party claim, action or allegation arising out of or relating to Contractor

Indemnified Parties' statements or communications to the media or other third-parties; and (ii) no indemnification obligations in connection with any third-party claim, action or allegation arising out of or relating to Contractor Indemnified Parties' material breach of this Agreement.

- 15.4 Indemnification Procedures. The Indemnified Party will (i) promptly notify the indemnifying party in writing of any claim, suit or proceeding for which indemnity is claimed, provided that failure to so notify will not remove the indemnifying party's obligation except to the extent it is prejudiced thereby, (ii) allow the indemnifying party to solely control the defence of any claim, suit or proceeding and all negotiations for settlement, and (iii) fully cooperate with the Indemnifying Party by providing information or documents requested by the Indemnifying Party that are reasonably necessary to the defense or settlement of the claim, and, at the Indemnifying Party's request and expense, assistance in the defense or settlement of the claim. In no event may either party enter into any third-party agreement which would in any manner whatsoever affect the rights of the other party or bind the other party in any manner to such third party, without the prior written consent of the other party. If and to the extent that any documents or information provided to the Indemnified Party would constitute Confidential Information within the meaning of this Agreement, the Indemnified Party agrees that it will take all actions reasonably necessary to maintain the confidentiality of such documents or information, including but not limited to seeking a judicial protective order.

This Article 15 states each party's exclusive remedies for any third-party claim or action, and nothing in the Agreement or elsewhere will obligate either party to provide any greater indemnity to the other. This Article 15 shall survive any expiration or termination of the Agreement.

16 FORCE MAJEURE

- 16.1 Neither party shall be liable to the other for failure to perform or delay in performance of its obligations under any Statement of Work if and to the extent that such failure or delay is caused by or results from causes beyond its control, including, without limitation, any act (including delay, failure to act, or priority) of the other party or any governmental authority, civil disturbances, fire, acts of God, acts of public enemy, compliance with any regulation, order, or requirement of any governmental body or agency, or inability to obtain transportation or necessary materials in the open market.
- 16.2 As a condition precedent to any extension of time to perform the Services under this Agreement, the party seeking an extension of time shall, not later than ten (10) days following the occurrence of the event giving rise to such delay, provide the other party written notice of the occurrence and nature of such event.

17 INSURANCE

During the of the Agreement Term, Contractor shall, at its own cost and expense, obtain and maintain in full force and effect, the following minimum insurance coverage: (a) commercial general liability insurance on an occurrence basis with minimum single limit coverage of \$2,000,000 per occurrence and \$4,000,000 aggregate combined single limit; (b) professional errors and omissions liability insurance with a limit of \$2,000,000 per event and \$2,000,000 aggregate; Contractor shall name Client as an additional insured to Contractor's commercial general liability and excess/umbrella insurance and as a loss payee on Contractor's professional errors and omissions liability insurance and Contractor's employee fidelity bond/crime insurance, and, if required, shall also name Client's End Customer. Contractor shall furnish to Client a certificate showing compliance with these insurance requirements within two (5) days of Client's written request. The certificate will provide that Client will receive ten (10) days' prior written notice from the insurer of any termination of coverage.

18 GENERAL

- 18.1 Independent Contractors-No Joint Venture. The parties are independent contractors and will so represent themselves in all regards. Neither party is the agent of the other nor may neither bind the other in any way, unless authorized in writing. The Agreement (including the Statements of Work) shall not be construed as constituting either Party as partner, joint venture or fiduciary of the other Party or to create any other form of legal association that would impose liability upon one Party for the act or failure to act of the other Party, or as providing either Party with the right, power or authority (express or implied) to create any duty or obligation of the other Party.
- 18.2 Entire Agreement, Updates, Amendments and Modifications. The Agreement (including the Statements of Work) constitutes the entire agreement of the Parties with regard to the Services and matters addressed therein, and all prior agreements, letters, proposals, discussions and other documents regarding the Services and the matters addressed in the Agreement (including the Statements of Work) are superseded and merged into the Agreement (including the Statements of Work). Updates, amendments, corrections and modifications to the Agreement including the Statements of Work may not be made orally but shall only be made by a written document signed by both Parties.
- 18.3 Waiver. No waiver of any breach of any provision of the Agreement shall constitute a waiver of any prior, concurrent or subsequent breach of the same or any other provisions hereof.
- 18.4 Severability. If any provision of the Agreement shall be held to be invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions shall not in any way be affected or impaired thereby, and such provision shall be deemed to be restated to reflect the Parties' original intentions as nearly as possible in accordance with applicable Law(s).
- 18.5 Cooperation in Defense of Claims. The parties agree to provide reasonable cooperation to each other in the event that either party is the subject of a claim, action or allegation regarding this Agreement or a party's actions taken pursuant to this agreement, including, but not limited to, providing information or documents needed for the defence of such claims, actions or allegation; provided that neither party shall be obligated to incur any expense thereby.

- 18.6 Counterparts. The Agreement and each Statement of Work may be executed in counterparts. Each such counterpart shall be an original and together shall constitute but one and the same document. The Parties agree that electronic signatures, whether digital or encrypted, a photographic or facsimile copy of the signature evidencing a Party's execution of the Agreement shall be effective as an original signature and may be used in lieu of the original for any purpose.
- 18.7 Binding Nature and Assignment. The Agreement will be binding on the Parties and their respective successors and permitted assigns. Neither Party may, or will have the power to, assign the Agreement (or any rights thereunder) by operation of law or otherwise without the prior written consent of the other Party.
- 18.8 Notices. Notices pursuant to the Agreement will be sent to the addresses below, or to such others as either party may provide in writing. Such notices will be deemed received at such addresses upon the earlier of (i) actual receipt or (ii) delivery in person, by fax with written confirmation of receipt, or by certified mail return receipt requested. A notice or other communication delivered by email under this Agreement will be deemed to have been received when the recipient, by an email sent to the email address for the sender stated in this Section 19.7 acknowledges having received that email, with an automatic "read receipt" not constituting acknowledgment of an email for purposes of this section 19.7.

Notice to Contractor:

Cyber Ninjas Inc
ATTN: Legal Department
5077 Fruitville Rd
Suite 109-421
Sarasota, FL 34232

Email: legal@cyberninjas.com

Notice to Client:

Arizona State Senate
Attn: Greg Jernigan
1700 W. Washington St.
Phoenix, AZ 85007
gjernigan@azleg.gov

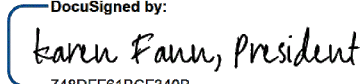
- 18.9 No Third-Party Beneficiaries. The Parties do not intend, nor will any Section hereof be interpreted, to create for any third-party beneficiary, rights with respect to either of the Parties, except as otherwise set forth in an applicable Statement of Work.

- 18.10 Dispute Resolution. The parties shall make good faith efforts to resolve any dispute which may arise under this Agreement in an expedient manner (individually, "Dispute" and collectively "Disputes"). In the event, however, that any Dispute arises, either party may notify the other party of its intent to invoke the Dispute resolution procedure herein set forth by delivering written notice to the other party. In such event, if the parties' respective representatives are unable to reach agreement on the subject Dispute within five (5) calendar days after delivery of such notice, then each party shall, within five (5) calendar days thereafter, designate a representative and meet at a mutually agreed location to resolve the dispute ("Five-Day Meeting").
- 18.10.1 Disputes that are not resolved at the Five-Day Meeting shall be submitted to non-binding mediation, by delivering written notice to the other party. In such event, the subject Dispute shall be resolved by mediation to be conducted in accordance with the rules and procedures of the American Arbitration Association, and mediator and administrative fees shall be shared equally between the parties.
- 18.10.2 If the dispute is not resolved by mediation, then either party may bring an action in a state or federal court in Maricopa County, Arizona which shall be the exclusive forum for the resolution of any claim or defense arising out of this Agreement. The prevailing party shall be entitled to an award of its reasonable attorneys' fees and costs incurred in any such action.
- 18.10.3 Governing Law. All rights and obligations of the Parties relating to the Agreement shall be governed by and construed in accordance with the Laws of the State of Arizona without giving effect to any choice-of-law provision or rule (whether of the State of Arizona or any other jurisdiction) that would cause the application of the Laws of any other jurisdiction.
- 18.11 Rules of Construction. Interpretation of the Agreement shall be governed by the following rules of construction: (a) words in the singular shall be held to include the plural and vice versa and words of one gender shall be held to include the other gender as the context requires, (b) the word "including" and words of similar import shall mean "including, without limitation," (c) the headings contained herein are for reference purposes only and shall not affect in any way the meaning or interpretation of the Agreement.

IN WITNESS WHEREOF, the parties hereto have caused this Master Service Agreement to be effective as of the day, month and year written above.

Accepted by:


Client

By:  DocuSigned by:
Karen Fann, President
748DEF61BCE340B

Title: Karen Fann, President

Accepted by:

Contractor: Cyber Ninjas, Inc.

By: 
Douglas Logan

Title: CEO & Principal Consultant

EXHIBIT 1. FORM OF STATEMENT OF WORK

This Statement of Work (the "Statement of Work") is effective as of as of the _____ day of _____, 20__ (the "Effective Date"), between Cyber Ninjas, Inc., a Florida Corporation, (the "Contractor"), and the Arizona State Senate (the "Client"), and is deemed to be incorporated into that certain Master Service Agreement dated the 31 day of March, 2021 (the "Master Agreement") by and between Contractor and Client(collectively, this Statement of Work and the Master Agreement are referred to as the "Agreement").

1 GENERAL PROVISIONS

- 1.1 Introduction. The terms and conditions that are specific to this Statement of Work are set forth herein. Any terms and conditions that deviate from or conflict with the Master Agreement are set forth in the "Deviations from Terms of the Master Agreement" Schedule hereto. In the event of a conflict between the provisions of this Statement of Work and the Master Agreement, the provisions of Section 2.4 of the Master Agreement shall control such conflict.
- 1.2 Services. Contractor will provide to the Client the Services in accordance with the Master Agreement (including the Exhibits thereto) and this Statement of Work (including the Schedules hereto). The scope and composition of the Services and the responsibilities of the Parties with respect to the Services described in this Statement of Work are defined in the Master Agreement, this Statement of Work, [and any Schedules attached hereto].

2 SCOPE & SERVICES DESCRIPTION

3 TECHNICAL METHODOLOGY

4 DELIVERABLE MATERIALS

5 COMPLETION CRITERIA

6 FEES / TERMS OF PAYMENT

The charges for the Services are: \$_____ to be paid as follows:

[\$_____ upon execution of the Agreement and \$_____ upon completion of the Services]. Invoicing and terms of payment shall be as provided in Article 5 of the Agreement.

7 TERM/PROJECT SCHEDULE

8 SIGNATURE & ACKNOWLEDGEMENT

THE PARTIES ACKNOWLEDGE THAT THEY HAVE READ THIS STATEMENT OF WORK, UNDERSTAND IT, AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS. FURTHER, THE PARTIES AGREE THAT THE COMPLETE AND EXCLUSIVE STATEMENT OF THE AGREEMENT BETWEEN THE PARTIES RELATING TO THIS SUBJECT SHALL CONSIST OF 1) THIS STATEMENT OF WORK, 2) ITS SCHEDULES, AND 3) THE AGREEMENT (INCLUDING THE EXHIBITS THERETO), INCLUDING THOSE AMENDMENTS MADE EFFECTIVE BY THE PARTIES IN THE FUTURE. THIS STATEMENT OF THE AGREEMENT BETWEEN THE PARTIES SUPERSEDES ALL PROPOSALS OR OTHER PRIOR AGREEMENTS, ORAL OR WRITTEN, AND ALL OTHER COMMUNICATIONS BETWEEN THE PARTIES RELATING TO THE SUBJECT DESCRIBED HEREIN.

IN WITNESS WHEREOF, the parties hereto have caused this Statement of Work to be effective as of the day, month and year written above.

Accepted by:

Client:

By: _____

Title: _____

Accepted by:

Contractor: Cyber Ninjas, Inc.

By: _____

Douglas Logan

Title: CEO & Principal Consultant

EXHIBIT 2. BACKGROUND SCREENING MEASURES

The pre-employment background investigations include the following search components for U.S. employees and the equivalent if international employees:

- 10-Year Criminal History Search – Statewide and/or County Level
- 10-Year Criminal History Search – U.S. Federal Level
- Social Security Number Validation
- Restricted Parties List

Criminal History – State-wide or County:

Criminal records are researched in the applicant's residential jurisdictions for the past seven years. records are researched through State-wide repositories, county/superior courts and/or lower/district/municipal courts. Generally, a State-wide criminal record search will be made in states where a central repository is accessible. Alternately, a county criminal record search will be conducted and may be supplemented by an additional search of lower, district or municipal court records. These searches generally reveal warrants, pending cases, and felony and misdemeanor convictions. If investigation and/or information provided by the applicant indicate use of an aka/alias, additional searches by that name must be conducted.

Criminal History – Federal:

Federal criminal records are researched through the U.S. District Court in the applicant's federal jurisdiction for the past seven years. This search generally reveals warrants, pending cases and convictions based on federal law, which are distinct from state and county violations. The search will include any AKAs/aliases provided or developed through investigation.

Social Security Trace:

This search reveals all names and addresses historically associated with the applicant's provided number, along with the date and state of issue. The search also verifies if the number is currently valid and logical or associated with a deceased entity. This search may also reveal the use of multiple social security numbers, AKAs/aliases, and additional employment information that can then be used to determine the parameters of other aspects of the background investigation.

Compliance Database or Blacklist Check:

This search shall include all of the specified major sanctioning bodies (UN, OFAC, European Union, Bank of England), law enforcement agencies, regulatory enforcement agencies, non-regulatory agencies, and high-profile persons (to include wanted persons, and persons who have previously breached US export regulation or violated World Bank procurement procedures including without limitation the lists specified below:

A search shall be made of multiple National and International restriction lists, including the Office of Foreign Asset Control (OFAC) Specially Designated Nationals (SDN), Palestinian Legislative Council (PLC), Defense Trade Controls (DTC) Debarred Parties, U.S. Bureau of Industry and Security Denied Persons List, U.S. Bureau of Industry and Security Denied Entities List, U.S. Bureau of Industry and Security Unverified Entities List, FBI Most Wanted Terrorists List, FBI Top Ten Most Wanted Lists, FBI Seeking Information, FBI Seeking Information on Terrorism, FBI Parental Kidnappings, FBI Crime Alerts, FBI Kidnappings and Missing Persons, FBI Televised Sexual Predators, FBI Fugitives – Crimes Against Children, FBI Fugitives – Cyber Crimes, FBI Fugitives – Violent Crimes: Murders, FBI Fugitives – Additional Violent Crimes, FBI Fugitives – Criminal Enterprise Investigations, FBI Fugitives – Domestic Terrorism, FBI Fugitives – White Collar Crimes, DEA Most Wanted Fugitives, DEA Major International Fugitives, U.S. Marshals Service 15 Most Wanted, U.S. Secret Service Most Wanted Fugitives, U.S. Air Force Office of Special Investigations Most Wanted Fugitives, U.S. Naval Criminal Investigative Services (NCIS) Most Wanted Fugitives, U.S. Immigration and Customs Enforcement (ICE) Most Wanted Fugitives, U.S. Immigration & Customs Enforcement Wanted Fugitive Criminal Aliens, U.S. Immigration & Customs Enforcement Most Wanted Human Smugglers, U.S. Postal Inspection Service Most Wanted, Bureau of Alcohol, Tobacco, and Firearms (ATF) Most Wanted, Politically Exposed Persons List, Foreign Agent Registrations List, United Nations Consolidation Sanctions List, Bank of England Financial Sanctions List, World Bank List of Ineligible Firms, Interpol Most Wanted List, European Union Terrorist List, OSFI Canada List of Financial Sanctions, Royal Canadian Mounted Police Most Wanted, Australia Department of Foreign Affairs and Trade List, Russian Federal Fugitives, Scotland Yard's Most Wanted, and the World's Most Wanted Fugitives.

EXHIBIT 3. FORM OF NONDISCLOSURE SUBCONTRACT

Nondisclosure Agreement

1. I am participating in one or more projects for Cyber Ninjas, Inc., as part of its audit of the 2020 general election in Maricopa County, performed as a contractor for the Arizona State Senate (the "Audit").
2. In connection with the foregoing, I have or will be receiving information concerning the Audit, including but not limited to ballots or images of ballots (whether in their original, duplicated, spoiled, or another form), tally sheets, audit plans and strategies, reports, software, data (including without limitation data obtained from voting machines or other election equipment), trade secrets, operational plans, know how, lists, or information derived therefrom (collectively, the "Confidential Information").
3. In consideration for receiving the Confidential Information and my participation in the project(s), I agree that unless I am authorized in writing by Cyber Ninjas, Inc. and the Arizona State Senate, I will not disclose any Confidential Information to any person who is not conducting the Audit. If I am required by law or court order to disclose any Confidential Information to any third party, I will immediately notify Cyber Ninjas, Inc. and the Arizona State Senate.
4. Furthermore, I agree that during the course of the audit to refrain from making any public statements, social media posts, or similar public disclosures about the audit or its findings until such a time as the results from the audit are made public or unless those statements are approved in writing from Cyber Ninjas, Inc and the Arizona Senate.
5. I agree never to remove and never to transmit any Confidential Information from the secure site that the Arizona State Senate provides for the Audit; except as required for my official audit duties and approved by both Cyber Ninjas, Inc and the Arizona Senate.
6. I further understand that all materials or information I view, read, examine, or assemble during the course of my work on the Audit, whether or not I participate in the construction of such materials or information, have never been and shall never be my own intellectual property.
7. I agree that the obligations provided herein are necessary and reasonable in order to protect the Audit and its agents and affiliates. I understand that an actual or imminent failure to abide by these policies could result in the immediate termination of my work on the Audit, injunctive relief against me, and other legal consequences (including claims for consequential and punitive damages) where appropriate.

Signature: _____

Printed Name: _____

Date: _____

Exhibit 3

**Cyber Ninjas**

Phone: (941) 3-NINJAS

Fax: (941) 364-6527

www.CyberNinjas.com

5077 Fruitville Rd #109-421, Sarasota, FL 34232

Statement of Work

This Statement of Work (the “Statement of Work”) is effective as of as of the 31 day of March, 2021 (the “Effective Date”), between Cyber Ninjas Inc., a Florida Corporation, (“Contractor”), and Arizona State Senate (“Client”), and is deemed to be incorporated into that certain Master Service Agreement dated March 31, 2021 (the “Master Agreement”) by and between Contractor and Client (collectively, this Statement of Work and the Master Agreement are referred to as the “Agreement”).

1 WHY CYBER NINJAS

Cyber Ninjas is a cyber security company with a focus on application security and ethical hacking. We perform work across the financial services and government sectors. Our expertise allows us to both understand complex technology systems, as well as understand how a malicious attacker could potentially abuse those systems to meet his or her own agenda. This allows us to effectively enumerate the ways a system could be exploited, and with our partners to fully review if that scenario did in fact occur. This is very different from the compliance focused way that election systems are typically evaluated.

Both our company and our partners have extensive experience working specifically with Dominion Voting Systems. In addition, our subcontractors and partners are adept at digital forensic acquisition, and on implementing ballot hand-counting procedures. Two of our team members authored a hand-count ballot process that has been utilized in audits in two states; and has further been perfected for transparency and consistency. This combination of skills, abilities, and experience is what uniquely qualifies our team for the outlined work.

2 OUR TEAM

Cyber Ninjas will serve as the central point-of-contact and organizer of all work conducted over the course of this agreement. However, there are different teams involved in each phase of the outlined work. Each of these teams have specialities and experience within the outlined areas of their coverage. This expertise is highlighted below.

2.1 Registration and Votes Cast Team

The Registration and Votes Cast Team has worked together with a number of individuals to perform non-partisan canvassing within Arizona related to the 2020 General election in order to statistically identify voter registrations that did not make sense, and then knock on doors to confirm if valid voters actually lived at the stated address. This brought forth a number of significant anomalies suggesting significant problems in the voter rolls.

They will be continuing this work as part of this effort to validate that individuals that show as having voted in the 2020 General election match those individuals who believe they have cast a vote.

2.2 Vote Count & Tally Team - Wake Technology Services

Members of the Wake Technology Services group have performed hand-count audits in Fulton County, PA and in New Mexico as part of the 2020 General Election cycle. In addition, team members have been involved in investigating election fraud issues, dating back to 1994. In that particular case in 1994, this team member worked closely with the FBI during the investigation.

As part of these audits in 2020, the Wake Technology Services team has developed an in-depth counting process that reduces opportunities for errors. This counting process has been expanded to make it more robust, and more transparent. As a result, they will be leading all ballot hand-counting processes.

2.3 Electronic Voting System Team – CyFIR, Digital Discovery & Cyber Ninjas, Analysts

Digital Forensic Acquisition will be performed either by CyFIR or Digital Forensics, and the analysis work will be performed by Cyber Ninjas, CyFIR and a number of additional analysts, the identities and qualifications of whom shall be made available to Client upon request.

CyFIR is a digital security and forensics company and a subcontractor on the contract for DHS's Hunt and Incident Response Team (HIRT). As specialists for DHS, they are familiar with responding to nation-state cyber activity including Advanced Persistent Threats (APT).

3 GENERAL PROVISIONS

- 3.1 Introduction. The terms and conditions that are specific to this Statement of Work are set forth herein. Any terms and conditions that deviate from or conflict with the Master Agreement are set forth in the "Deviations from Terms of the Master Agreement" Schedule hereto. In the event of a conflict between the provisions of this Statement of Work and the Master Agreement, the provisions of Section 2.34 of the Master Agreement shall control such conflict.
- 3.2 Services. Contractor will provide to the Client the Services in accordance with the Master Agreement (including the Exhibits thereto) and this Statement of Work (including the Schedules hereto). The scope and composition of the Services and the responsibilities of the Parties with respect to the Services described in this Statement of Work are defined in the Master Agreement, this Statement of Work, and any Schedules attached hereto.

4 SCOPE & SERVICES DESCRIPTION

This Statement of Work outlines the proposed methodology and scope for a full and complete audit of 100% of the votes cast within the 2020 November General Election within Maricopa County, Arizona. This audit will attempt to validate every area of the voting process to ensure the integrity of the vote. This includes auditing the registration and votes cast, the vote counts and tallies, the electronic voting system, as well as auditing the reported results. The final report will attempt to outline all the facts found throughout the investigation and attempt to represent those facts in an unbiased and non-partisan way. The final report will not include factual statements unless the statements can be readily substantiated with evidence, and such substantiation is cited, described, or appended to the report as appropriate.

The following sub-sections provides additional details of what will be conducted at each stage of the audit.

4.1 Registration and Votes Cast Phase

During the Registration and Votes Cast Phase, it will be validated that Maricopa County properly registers who voted during an election, and that this system properly prevents duplicate voting. This will be performed on a minimum of three precincts.

Proposed scope of work:

- Review of Arizona's SiteBook system for checking in and tracking voters;
- Complete audit of a minimum of 3 precincts, based on statistical anomalies and precinct size;
- Analysis of existing research and data validating the legitimacy of voter rolls; and/or
- Comparing results against known lists of invalid voters (e.g. deceased voters, non-citizens, etc.).

This phase may help detect:

- Problems that could result in voters being able to vote more than once;
- Voters that voted but do not show in the list of those who voted;
- Voters who likely did not vote but showed as having voted;
- Potential invalid voters who cast a vote in the 2020 general election; and/or
- Inconsistencies among vote tallies between the various phases.

This phase is NOT expected to detect:

- Individual ballots that are either wrong and/or invalid.

Anticipated artifacts for transparency and/or validation of results for the public:

- Final report outlining the discovered results; and/or
- Redacted spreadsheet of a list of those who voted in the target precincts.

4.2 Vote Count & Tally Phase

During the Vote Count & Tally Phase, the counts and tallies for votes and the voting machines will be validated. This will include a hand-tally and examination of every paper ballot.

Proposed scope of work:

- Physically inspecting and hand-counting of ballots in Maricopa County;
- Counting of the total number of provisional ballots;
- Capture of video footage of the hand-counting of ballots; and/or
- Scanning of ballots in Maricopa County
 - NOTE: Provisional ballots which still have signatures attached to them will be counted to be sure they match the expected numbers but will not be scanned nor will the contents be visible in video.

This phase may help detect:

- Counts that do not match the expected results;
- Ballots that are visually different and possibly fraudulent; and/or
- Inconsistencies among vote tallies between the various phases.

This phase is NOT expected to detect:

- Destroyed or otherwise missing ballots

Anticipated artifacts for transparency and/or validation of results for the public:

- Final report outlining the discovered results;
- Unedited camera footage of the counting of every ballot, provided that, absent express judicial approval, any such footage cannot be streamed, recorded or broadcast in such a manner that the candidate or ballot proposition selections on each ballot is visible or discernible; and/or
- Ballot images of every scanned ballot, provided that, absent express judicial approval, any such images cannot be released or published to any third party.

4.3 Electronic Voting System Phase

During the Electronic Voting System Phase the results from the electronic voting machines will be validated to confirm they were not tampered with. This will be done on all systems related to SiteBook with Maricopa data, as well as all Election Management System related machines besides the Ballot Marking Devices (BMD)'s utilized for accessibility.

Proposed scope of work:

- Forensic Images of Arizona's SiteBook System including the database server, as well as any client machines associated with Maricopa County;
- Forensic images captured of the Election Management System main server, adjudication machines, and other systems related to the Election Management System;
- Forensic images of all Compact Flash, USB drives, and related media;
- Inspection to identify usage of cellular modems, Wi-Fi cards, or other technologies that could be utilized to connect systems to the internet or wider-area-network;
- Review of the Tabulator Paper Tally print-outs;
- Reviewing the exports from the EMS for "Audit File", "Audit Images" and "CVR";
- Reviewing ballot images captured by the tabulators
- Reviewing forensic images for possible altering of results or other issues; and/or
- Reviewing of tabulator and other logs.

This phase may help detect:

- Problems where the tabulator incorrectly tabulated results;
- Problems where the tabulator rejected results;
- Issues where results may have been manipulated in the software;
- Issues with the improper adjudication of ballots; and/or
- Inconsistencies among vote tallies between the various phases.

Anticipated artifacts for transparency and/or validation of results for the public:

- Final report outlining the discovered results;
- Ballot images and AuditMark images showing how the tabulator interpreted the ballot for counting, provided that, absent express judicial approval, such images cannot be released or published to any third party;
- CVR Report as generated from the software; and/or
- Log Files from the Tabulators (Redacted if Dominion Desires).

4.4 Reported Results Phase

During the Reported Results Phase, results from all phases are compared against those expected results and those results which were publicly totalled as the official results to identify any inconsistencies.

Proposed scope of work:

- Results from various phases will be reviewed and tallied; and
- Results will be compared against the official, certified results.

This phase may help detect:

- Issues where result tallies were not properly transmitted to the official results; and/or
- Inconsistencies among vote tallies between the various phases.

Anticipated artifacts for transparency and/or validation of results for the public:

- Final report outlining the discovered results

5 METHODOLOGY

The following section outlines the proposed methodology utilized in the various phases of the audit. When appropriate, these sections may reference more detailed procedures. Such procedures are considered proprietary and the intellectual property of Cyber Ninjas, our subcontractors or our Partners and can be made available for review but are not explicitly part of this agreement.

5.1 Registration and Votes Cast Phase

During the “Registration and Votes Cast Phase”, Contractor may utilize precincts that have a high number of anomalies based on publicly available voting data and data from prior canvassing efforts to select a minimum of three precincts to conduct an audit of voting history related to all members of the voter rolls. A combination of phone calls and physical canvassing may be utilized to collect information of whether the individual voted in the election. No voters will be asked to identify any candidate(s) for whom s/he voted. This data will then be compared with data provided from Maricopa County Board of Elections.

5.2 Vote Count & Tally Phase

The goal of the “Vote Count & Tally Phase” is to attempt to, in a transparent and consistent manner, count all ballots to determine the accuracy of all federal races, and to identify any ballots that are suspicious and potentially counterfeit. Ballots will be counted in a manner designed to be accurate, all actions are transparent, and the chain of custody is maintained.

5.2.1 Counting Personnel

Non-partisan counters will be utilized that are drawn from a pool of primarily former law enforcement, veterans, and retired individuals. These individuals will undergo background checks and will be validated to not have worked for any political campaigns nor having worked for any vendor involved in the voting process. These individuals will also be prevented from bringing any objects other than clothing items worn on their persons into the counting area or taking any objects out of the counting area.

5.2.2 Accurate Counting

Counting will be done in groups with three individuals independently counting each batch of ballots, and an individual supervising the table. All counts will be marked on a sheet of paper as they are tallied. If, at the end of the hand count, the discrepancies between counting personnel aggregate to a number that is greater than the margin separating the first and second place candidates for any audited office, the ballots with discrepant total from the Contractor's counting personnel will be re-reviewed until the aggregate discrepancies within the hand count are less than the margin separating the first and second place candidates.

5.2.3 Transparent Counting

All activity in the counting facility will be videotaped 24 hours a day, from the time that Maricopa County delivers ballots and other materials until the time that the hand count is complete and all materials have been returned to the custody of Maricopa County. Such videotaping shall include 24-hour video monitoring of all entrances and exits, as well as activity at the counting tables.

5.2.4 Chain of Custody

All movement with ballots, cutting of seals, application of seals, and similar actions will be appropriately documented and logged, as well as captured under video to be sure the custody of ballots is maintained at all times. Access to the counting area will be restricted to duly authorized and credentialed individuals who have passed a comprehensive background check, with mandatory security searches and ingress/egress logs whenever entering or exiting the counting area.

5.3 Electronic Voting System Phase

The proposed scope of the "Electronic Voting System Phase" is to confirm that the system accurately tallied and reported the votes as they were entered into the system and that remote access was not possible. All systems related to the voting will be forensically imaged, these machines will be booted up and checked for wireless signal usage, and the images will be reviewed to determine the accuracy of results and any indication of tampering.

5.3.1 Forensic Images

A digital forensics capture team will forensically capture all data on in-scope systems, utilizing industry best practices. This will create a digital copy of every single machine, Compact Flash Card, and USB drive in scope without altering the contents of the machines. Chain-of-custody documentation will be created to preserve these images in a manner sufficient to be utilized in a court-of-law.

5.3.2 Physical Analysis

The Election Management System equipment will be turned on and scanned with a wireless spectrum analysis tool to determine if the device is emitting any signals consistent with a known wireless frequency such as cellular, Bluetooth, WiFi or similar. Devices that show signs of emitting signals will be flagged and documented, and when possible without damaging the equipment; they will be physically inspected to determine the source of any detected signals.

5.3.3 Digital Analysis

The forensic images will be reviewed to validate reported totals from the tabulators, results stored within the Election Management System (EMS) Results Tally and Reporting software. These will be compared against the tabulator print-outs; and the machine will be checked for physical or digital tampering and any known ways of remote access to the machines.

5.3.4 Opportunity for Observation

Before commencing the imaging or analysis steps described above (except for the Digital Analysis process), the Contractor will work with Maricopa County to provide at least five (5) days advance notice to any vendors of Maricopa County whose products will be the subject of imaging, inspection, or analysis. Such vendors will be permitted the opportunity to attend and observe the Contractor's imaging or inspection of the vendors' products. The vendor will not be allowed to be present for the analysis of the captured images. Such vendors are third party beneficiaries of this provision and will have standing to challenge and secure injunctive relief against any denial of their right to observe the inspection of their products.

5.4 Reported Results Phase

During the Reported Results phase, results from all phases are compared to find differences between tallies or other anomalies. These results are then compared against data at the Secretary of State and Maricopa Board of Elections layers. Any inconsistencies will be reported and highlighted.

6 RESPONSIBILITIES

The following section outlines the key responsibilities for the proper execution of the Agreement between the Contractor and the Client for all outlined work within the scope.

6.1 Registration and Votes Cast Phase

Contractor Responsibilities

- Provide the proper personnel to conduct the analysis of the data required to execute the scope of this phase.

Client Responsibilities

- Arrange for a database export of SiteBook to be provided to the Client which includes all fields normally found in a publicly requested copy of the voter rolls, in addition to any other non-sensitive fields related to the data such as modifications or other time-stamps, voter history, last user edited, IP address of edit; or anything similar.

6.2 Vote Count & Tally Phase

Contractor Responsibilities

- Provide the proper personnel and equipment to execute all aspects of the phase including scanning, counting, the setup of equipment for recording of the counting, and the supervision of activities.
- Ensure that all onsite personnel follow any in-place COVID requirements.

Client Responsibilities

- Provide security of the building during the course of the engagement. This includes having sufficient security to prevent access to the building 24/7 during the entire time, including ensuring that safe working conditions can exist during the entirety of the audit;
- Provide electricity and access to the facilities and tables necessary for up to 120 people at a time following any current COVID requirements. This is estimated to be about 7,200 square feet;
- Provide access to all paper ballots from the November 2020 General Election within Maricopa County. This includes early voting, election day ballots, provisional ballots, spoiled ballots, printed unused ballots and any other ballot categories that are part of the 2020 General Election. For all ballots this should include the original hard copies of the ballots that were electronically adjudicated ballots.
- Provide a mechanism to allow for the proper equipment to be brought into the facility where the counting will take place.

- Full chain of custody documentation for all ballots from the point they were cast to the point where we gain access to the ballots, to the extent such documentation is in Client’s possession.
- Purchase orders for all purchased ballots, or ballot paper, including counts of each, as well as delivery receipts of the quantity of ballots received, to the extent such documentation is in Client’s possession.
- Full counts from any ballots printed on demand, as well as the location for which they were printed, to the extent such documentation is in Client’s possession.
- Provide wired access to internet to be able to stream the counting video capture, provided that any such video footage must be streamed, recorded or broadcast in such a manner that the candidate or ballot proposition selections on each ballot shall not be visible or discernible.

6.3 Electronic Voting System Phase

Contractor Responsibilities

- Provide the proper personnel to execute all aspects of the phase including the capture of forensic digital images of all systems related to the Election Management System; and
- Ensure that all onsite personnel during the forensic capture follow any in-place COVID requirements.

Client Responsibilities

- Provide physical access to the EMS Server, Adjudication machines, ImageCast Central, ImageCast Precinct, ImageCast Ballot Marking Devices, SiteBook, NOVUS systems, and any other Election Management System equipment or systems utilized in the November 2020 General Election to the forensic capture team;
- Provide access to Compact Flash Cards, USB Drives, and any other media utilized in the November 2020 General Election for the forensic capture team to image;
- Provide electricity and sufficient access to the machines in scope in order to provide a team of up to 15 forensic capture individuals to work and boot up the systems;
- Provide any needed credentials for decrypting media, decrypting computer hard drives, the EMS machines, or other systems that may be required for a proper forensic capture of the machines;
- Provide the output of the “Audit File,” “Audit Images,” and CVR exports from the Dominion machines which includes all ballot images and AuditMark images of every ballot processed by the machines; and
 - NOTE: The above may be able to be captured from the forensic images; but Maricopa County assistance could be needed in identifying where the AuditMark files are located.
- Provide any needed technical assistance allowing all the above to be successfully captured.

6.4 Reported Results Phase

Contractor Responsibilities

- Provide the proper personnel to conduct the analysis of the data required to execute the scope of this phase.

Client Responsibilities

- Provide the official results per precinct for all counts associated with the November 2020 General Election.

7 DELIVERABLE MATERIALS

The primary deliverable for the Election Audit will be a report detailing all findings discovered during the assessment. The parties agree that the report is provided AS IS, without any promise for any expected results. Additional artifacts as collected during the work will also be provided, as outlined within the scoping details.

This final report will include:

- An executive summary outlining the overall results of the audit from the various phases;
- A methodology section outlining in detail the methodology and techniques utilized to capture and validate the results;
- Tables, charts, and other data representing the findings of the data;
- Appendices or attached files demonstrating all evidence utilized to come to the outlined conclusions (if applicable); and
- Recommendations on how to prevent any detected weaknesses from being a problem in future elections (if applicable).

In addition to the report, various anticipated artifacts for public consumption will be generated over the course of this work, as outlined under the "Scope of Work." Client will determine in its sole and unlimited discretion whether, when, and how the Contractor should release those resources to the public. This will include all videos, ballot images, and other data.

8 COMPLETION CRITERIA

Contractor shall have fulfilled its obligations when any one of the following first occurs:

- Contractor accomplishes the Contractor activities described within this Statement of Work, including delivery to Client of the materials listed in the Section entitled "Deliverable Materials," and Client accepts such activities and materials without unreasonable objections; or
- If Client does not object or does not respond to Contractor within seven (7) business days from the date that the deliverables have been delivered by Contractor to Client, such failure to respond shall be deemed acceptance by Client.

9 TERM / PROJECT SCHEDULE / LOCATION

The following table outlines the expected duration of the various proposed work outlined within the Agreement. Work will commence on a date mutually agreeable to both Contractor and Client according to a schedule which is outlined via email.

Each phase outlined below can be conducted simultaneously, with the exception of the Reported Results phase which must be completed at the end. Roughly an additional week of time at the conclusion of all phases is needed to complete and finalize reporting. Lead times before a phase can start as well as their duration can be found below. Faster lead times can potentially be accommodated on a case-by-case basis.

Service Name	Required Notice / Lead Time	Est. Duration in Days	Additional Details / Location
Registration and Votes Cast Phase	1 Week	20	This work will be done remotely.
Vote Count & Tally Phase	2-3 Weeks	20*	The entire time will be onsite at the location designated by the Client. Access will be required 4 days before the start to setup the space. *Race recounts as outlined in 5.2.2 may require the timeline to be extended beyond the listed days.
Electronic Voting System Phase	1-2 Weeks	35	It is estimated that 15 will be onsite. The remainder of the time will be remote. Review of location setup is requested the week prior to ensure proper workspace.
Reported Results Phase	Completion of Other Phases	5	This phase will be completed offsite. Final Report Delivered 1 Week After Completion

10 FEES / TERMS OF PAYMENT

The following table outlines the costs associated with the proposed work. A third of the fees will be due at the execution of the contract. The remaining balance will be payable within 30 days from the completion of the audit.

Selected	Name	Price Each	Total
1	Maricopa County – Full Audit	\$150,000	\$150,000.00
		Total:	\$150,000.00

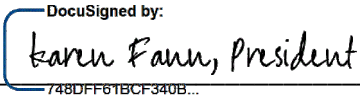
11 SIGNATURE & ACKNOWLEDGEMENT

THE PARTIES ACKNOWLEDGE THAT THEY HAVE READ THIS STATEMENT OF WORK, UNDERSTAND IT, AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS. FURTHER, THE PARTIES AGREE THAT THE COMPLETE AND EXCLUSIVE STATEMENT OF THE AGREEMENT BETWEEN THE PARTIES RELATING TO THIS SUBJECT SHALL CONSIST OF 1) THIS STATEMENT OF WORK, 2) ITS SCHEDULES, AND 3) THE AGREEMENT (INCLUDING THE EXHIBITS THERETO), INCLUDING THOSE AMENDMENTS MADE EFFECTIVE BY THE PARTIES IN THE FUTURE. THIS STATEMENT OF THE AGREEMENT BETWEEN THE PARTIES SUPERSEDES ALL PROPOSALS OR OTHER PRIOR AGREEMENTS, ORAL OR WRITTEN, AND ALL OTHER COMMUNICATIONS BETWEEN THE PARTIES RELATING TO THE SUBJECT DESCRIBED HEREIN.

IN WITNESS WHEREOF, the parties hereto have caused this Statement of Work to be effective as of the day, month and year written above.

Accepted by:

Client: Arizona State Senate

By:  DocuSigned by:
Karen Fann, President
748DFF61BCF340B...

Title: Karen Fann, President

Accepted by:

Contractor: Cyber Ninjas, Inc.

By: 

Douglas Logan

Title: CEO & Principal Consultant