

## Response to RFP for STAR-Vote™: A New Voting System

<i>RFP #</i>	P1609-008-LC
<i>RFP Subject</i>	STAR-Vote™: A New Voting System for Travis County, Texas
<i>Proposer's Name</i>	Galois, Inc., DBA Free & Fair
<i>Type of Organization</i>	Other Small Business
<i>Technical Point of Contact</i>	Dr. Joseph Kiniry 421 SW Sixth Avenue, Suite 300 Portland, OR 97204 503.808.7228, <a href="mailto:kiniry@freeandfair.us">kiniry@freeandfair.us</a>
<i>Administrative Point of Contact</i>	Jodee LeRoux 421 SW Sixth Avenue, Suite 300 Portland, OR 97204 ph 503.808.7209, <a href="mailto:contracts@galois.com">contracts@galois.com</a>
<i>Date Proposal Prepared</i>	January 26, 2017

# Table of Contents

## Primary Sections

Transmittal Letter/Executive Summary .....	1
Detailed Proposal .....	2
Cost Proposal/Schedule of Items .....	71
Proposer References.....	72
Description of Proposer .....	77
Description of Typical Engagements.....	78
Proposer Representative.....	79
Ethics Affidavit.....	80
HUB Program Subcontracting Declaration .....	81
Qualifications Questionnaire/Firm Experience and Qualifications .....	82
Insurance Requirements.....	83

## Detailed Proposal Sections

1	Overview .....	2
2	Part I, 1.0 General Requirements .....	8
3	Part II, 2.0 Detailed Response: Project Management .....	9
4	Part II, 5.0 Detailed Response: Element B .....	24
5	Part II, 6.0 Detailed Response: Element C .....	44
6	Part II, 9.0 Contractor Requirements .....	52
7	Part II, 10.0 Contract Requirements .....	52
8	Part II, 11.0 Maintenance/Service Level Requirements .....	52
9	RFP Appendix B: In-Person Voting/Tabulation.....	52
10	RFP Appendix C: Support Modules .....	55
11	RFP Appendix D: Software Specification .....	55
12	RFP Appendix E: Cryptography .....	56
13	RFP Appendix F: Hardware Requirements .....	58
14	RFP Appendix G: Procedures, Manuals, Instructions, and Training.....	61
15	RFP Appendix H: Data Specifications .....	61
16	Proposal Appendix 1: Project Storytelling .....	64
17	Proposal Appendix 2: Bios of Selected Team Members .....	66

## **Transmittal Letter/Executive Summary**

## FREE & FAIR

January 26, 2017

Travis County  
RFP P1609-008-LC  
STAR-Vote: A New Voting System

By developing the STAR-Vote specification and issuing Request for Proposal #P1609-008-LC (the RFP), Travis County has staked out a bold leadership position as the United States makes the inevitable transition from proprietary, black-box voting systems owned by vendors to transparent voting systems owned by citizens and government.

Free & Fair is pleased to respond to Elements B and C of Travis County RFP #P1609-008-LC: "STAR-Vote™: A New Voting System". Our proposal allows Travis County to choose to award any subset of our responses.

We propose many innovative ideas to support Travis County's goals, such as Virtual Reality to demonstrate and test products early during development, a superior variant of the cryptographic protocol, and the use of a Project Storyteller to help the public, especially other counties, voters and the Open Source community, better understand Travis County's vision for STAR-Vote.


Free & Fair's mission is to bring open source, high-assurance, end-to-end verifiable elections to the world. In this response to the RFP, Free & Fair proposes to create the world's most usable, accessible, trustworthy, and secure voting system for Travis County. The system will fulfill the technical requirements stipulated in last year's RFI and the current RFP and, taking into account the recently-released Statement of Interest (SOI) addendum to this RFP, leverage as much existing quality technology (commercial or open source) as possible.

Free & Fair is exactly the right entity to realize Travis County's bold vision of STAR-Vote because we have:

- world-class expertise in high assurance open source elections systems,
- an unparalleled record in delivering high assurance tools and systems to the most demanding clients in the USA on time and within budget,
- vast experience with creating, contributing to, and managing Open Source Software, and a deep knowledge of Open Source licenses and business cases, and
- corporate principles that are deeply aligned with those of the County. The STAR-Vote project's success breeds our success, and our success reinforces STAR-Vote's success.

We are committed to perform the work outlined in this proposal and hope to have the opportunity to work with Travis County on this important endeavor.

Regards,



Joseph Kiniry, Ph.D., CEO & Chief Scientist

## Detailed Proposal

### 1 Overview

By developing the STAR-Vote specification and issuing Request for Proposal #P1609-008-LC (the RFP), Travis County has staked out a bold leadership position as the United States makes the inevitable transition from proprietary, black-box voting systems owned by vendors to transparent voting systems owned by citizens and government.

We are pleased to respond to Elements B and C of Travis County RFP #P1609-008-LC: “STAR-Vote™: A New Voting System.” Our proposal allows Travis County to choose to award any subset of our responses. The systems we propose to create are:

- Element B: In-Person Voting/Tabulation and Support: \$4M, with delivery in 18 months from start of contract.
- Element C (Option 1): Ballot Box/Scanner: \$817K, with delivery of design in 18 months from start of contract.

We propose many innovative ideas to support Travis County’s goals, such as Virtual Reality to demonstrate and test products early during development, a superior variant of the cryptographic protocol, and the use of a Project Storyteller to help the public, especially other counties, voters and the Open Source community, better understand Travis County’s vision for STAR-Vote.

#### 1.1 Free & Fair:<sup>1</sup> The Dream Partner for Travis County and STAR-Vote

Free & Fair’s mission is to bring open source, high-assurance, end-to-end verifiable elections to the world. In this response to the RFP, Free & Fair proposes to create the world’s most usable, accessible, trustworthy, and secure voting system for Travis County. The system will fulfill the technical requirements stipulated in last year’s RFI and the RFP and, taking into account the recently-released Statement of Interest (SOI) addendum to the RFP, leverage as much existing quality technology (commercial or open source) as possible.

Free & Fair is exactly the right entity to realize Travis County’s bold vision of STAR-Vote because we have:

- world-class expertise in high assurance open source elections systems,
- an unparalleled record in delivering high assurance tools and systems to the most demanding clients in the USA on time and within budget,
- vast experience with creating, contributing to, and managing Open Source Software, and a deep knowledge of Open Source licenses and business cases, and
- corporate principles that are deeply aligned with those of the County. The STAR-Vote project’s success breeds our success, and our success reinforces STAR-Vote’s success.

We reflect upon these points in the following pages of this Executive Summary.

---

<sup>1</sup> Galois, Inc. produces hardware and software for a variety of applications. For election-related products, Galois operates under the name Free & Fair.

Our world-class expertise is concretized in three main dimensions relevant to STAR-Vote:

- Free & Fair has, in aggregate, nearly 100 years of open source experience spanning over 100 open source projects, including experience resolving the security issues raised by use of COTS hardware.
- Free & Fair staff have been involved with, or are the originators of, some of the most influential, high-profile open source projects in the world. The breadth of our work is remarkable, and includes the world's most popular operating system (Linux, used in Android phones and many other consumer electronics devices), libraries for secure communication and storage (e.g., SSL libraries and cryptography on many recent LG smartphones), programming languages (e.g., Java, Fortran, and Eiffel), programmer tools (e.g., Emacs, Eclipse, and numerous plugins to modern IDEs), compilers (e.g., the GNU compiler toolchain and the clang/LLVM toolchain), graphics (e.g., Mesa, the library which provides 3D rendering on many platforms), and a plethora of tools used for teaching about and building high assurance systems (OpenJML, ESC/Java2, EBON, Cryptol, SAW, and more).
- Our CEO and Chief Scientist, Dr. Joseph Kiniry, is widely known in the elections integrity and scientific community for his fifteen years of work pursuing a vision of high assurance election systems for trustworthy democracy.

Another strength is our ability to attract and manage world-class subcontractors. We have obtained commitments from notable experts such as Drew Davies, the founder of Oxide Design (creators of the Anywhere Ballot); Emmy-winning designer Jon Levy of AMA Studios; Morgan Miller, one of the few usable security experts with elections experience; internationally recognized formal verification technology expert David Cok; world-famous election systems security expert Harri Hursti; Maggie MacAlpine, a world leader in risk limiting audits; and cryptographer Douglas Wikström, founder of Verificatum AB, who is widely regarded as the world's top expert in mix-nets as applied to elections.

More information on our team members is available in Section 17.

## 1.2 On Time and Within Budget

Free & Fair's principals and this project team have ample experience delivering provably secure technology to government, on time and on budget. In particular, all projects listed in the Qualifications Questionnaire were delivered on time and on budget.

Free & Fair is already deeply familiar with STAR-Vote. We expect to develop the system quickly based on our experience developing Free & Fair's existing products and demonstrator components, which already implement much of the functionality of the Elements we propose. Over the past year we have developed prototype elections technologies including a STAR-Vote demonstrator, an electronic poll book, a verifiable in-person voting system, and tabulation and auditing software. We have used these prototypes to enhance our understanding of the state-of-the-art in elections technology and to demonstrate the style and quality of our software development capabilities. Our existing STAR-Vote demonstrator fulfills many of Element B's requirements. Since these prototypes were not designed for high assurance, nor for use in large-scale production environments, they will not be part of the proposed system. However, our experience developing them will speed our development of the proposed STAR-Vote system.



We expect to cut certification times in half by providing design, code, validation and verification artifacts immediately to the certification authority. While we cannot dictate the timelines of independent certification authorities, our development methods produce a comprehensive set of certification artifacts as part of the design and implementation process, so there is no delay between the end of development and the submission of complete materials to the certification authority. An example of this approach is the election tabulation system built by a team led by Dr. Kiniry and used in The Netherlands for the 2004 European Council Elections. This system was developed and certified within 12 calendar weeks instead of the year or more typical for election systems in that country at that time.<sup>2</sup>

### 1.3 Open Source Veterans

Traditionally, election technology vendors have profited from limited competition and retaining ownership of proprietary systems. Free & Fair has a different business model. Free & Fair understands the budget constraints that jurisdictions face, and welcomes the opportunity to be a partner in finding ways to control costs by using COTS hardware and open source software, allowing competition into every aspect of election technology. In particular:

- All software we have developed and that we propose to the client is open source, which allows inspection by any person interested in assuring or improving the security or functions of the voting system.
- All hardware proposed is either COTS or, where custom hardware is required, open hardware, allowing Travis County to benefit from open competition among vendors.
- In order to widen Travis County's future hardware options, and to encourage a wide community of STAR-Vote users, all proposed software will be capable of running on all mainstream operating systems (Microsoft Windows, Apple macOS, and various Linux flavors).

### 1.4 Security for "Critical Infrastructure"

In preparation for the 2016 presidential election, nearly every state requested help from the U.S. Department of Homeland Security (DHS) to secure election technology. Events such as these requests, and inquiries following the election, have raised public awareness of the importance of security to election administration. Even without a malicious attack, every Election Day brings stories of bugs and glitches that cause a public outcry somewhere, especially if the number of votes affected comes close to a margin of victory. More than ever before, election officials have been asked to assure the public that their elections have been run correctly. In January 2017, in response to the increasing sophistication of adversaries who might wish to attack or disrupt U.S. elections, DHS officially designated U.S. elections systems "critical infrastructure" on par with systems vital to energy, financial services, healthcare, transportation, agriculture, and communications.

The Free & Fair principals have treated democracy and election systems as critical systems and infrastructure for decades in our work with other governments and in R&D projects on election systems.

---

<sup>2</sup> For more detail, see Section 4.7.2.

We propose to build election technology for Travis County that meets the highest federal standards for software design and security from the National Institute of Standards and Technology (NIST). Most common commercial computing systems depend on “recovery” from occasional crashes (if the screen freezes, just restart it!), but the software development techniques specified by NIST have proven effective for building software **without bugs**. While these techniques may be new to the election community, key members of the Free & Fair project team have used them for 17 years in government contracts worth \$160M. We have developed products for governments and secured those products against persistent threats from nation-state actors (such as Russia and North Korea) and insider attacks. Free & Fair proposes not merely to fulfill the STAR-Vote requirements, but to fulfill the requirements with systems as secure as the other systems currently designated “critical infrastructure” by DHS.

NIST Special Publication 800-160<sup>3</sup> specifies **high-assurance systems**, also called **trustworthy systems**. These systems are designed from first principles to be free of flaws, including ones related to system correctness, security, reliability, assurance, and more. High-assurance systems are used in situations where failure can lead to loss of life (e.g., an automated train) or have enormous financial implications (e.g., digital cash in smart cards).

Free & Fair project team members have successfully developed many high assurance systems (examples include projects referenced in the Qualifications Questionnaire below, such as GULPHAAC) that face many of the same challenges (correctness, security, usability, accessibility, etc.) and use the same technologies (operating systems, programming languages, distributed systems, cryptography, etc.) required by elections systems. Our development process and methodology—cited prominently in NIST Interagency Report 8151,<sup>4</sup> written for the White House—includes strict adherence to design, code, and documentation standards, provides easily verifiable evidence for implementation correctness and security, and incorporates the writing and generation of comprehensive test suites for every component of the system. Free & Fair will bring the high assurance of safety and mission-critical systems to the elections systems and services market, at low cost, and with publicly owned open source technology on COTS hardware.

## 1.5 Deployment Track Record

Over the past fifteen years, Free & Fair staff members have consistently created and supported critical technology products. We have a track record of productizing, deploying, and continuously maintaining complex, secure, high-assurance technologies. Some of the highlights that illustrate our history of deploying and maintaining highly advanced, often open source systems, used by some of the biggest organizations in the world include:

- **High Assurance Cyber Military Systems (HACMS):** Tools to generate provably secure code for vehicles. Used by Boeing to “hack-proof” the unmanned Little Bird.
- **CyberChaff:** Advanced network defense system that leverages distraction and obfuscation. Deployed by a Fortune 50 company and at universities.

---

<sup>3</sup> NIST Special Publication 800-160: *Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, <https://doi.org/10.6028/NIST.SP.800-160>

<sup>4</sup> NIST Interagency Report 8151: *Dramatically Reducing Software Vulnerabilities*, <https://doi.org/10.6028/NIST.IR.8151>



- **Copilot:** Software to detect and report critical hardware failures before they cause accidents. Funded and deployed at NASA.
- **Cryptol:** Toolset to create and verify encryption software. Funded by NSA and deployed across the US government.
- **Software Analysis Workbench:** Toolset to help scientists and engineers formally verify computer programs and establish provable correctness and security guarantees. Deployed by Amazon to provably guarantee the security of encryption software.

We describe these projects in detail under Firm Experience in the Qualifications Questionnaire.

## 1.6 Choice of Cryptographic Protocol

Travis County may choose between the cryptographic protocol defined in the STAR-Vote RFP (the “STAR-Vote Protocol”) and what we argue is a more robust, more development-time-efficient variant (the “STAR-Vote Mix-Net Protocol”). We discuss this design choice in detail in our response to Appendix E: Cryptography. These two approaches are essentially cost neutral, but the implementation timeline of using the latter protocol is expedited.

## 1.7 Virtual Reality

Virtual Reality (VR) systems allow you to view and interact with computer generated environments as if you are actually in them. Recent systems, such as the HTC Vive that we use at Free & Fair, allow for full physical movement and direct interaction with elements within the environment.

For the STAR-Vote project, VR will give project participants and stakeholders the opportunity to physically experience the voting system under development. Instead of waiting until the system design is finalized, election officials and others can test the design in time to make actionable suggestions for improvement. Election administrators can use VR to catch design issues and rapidly verify that they have been fixed, and interested members of the public and the county commission can directly witness the system in operation before a dollar is spent on hardware for deployment.

All of these interactions will happen in a virtual room that is shared between Free & Fair and Travis County, allowing us to talk, gesture, and interact as if we are standing in the same polling place. Instead of needing to know how to use complex design software, an election administrator can simply (virtually) walk up to and use a prototype voting machine. To examine a specific spot more carefully there is no need to “zoom in”; instead, you do just what you would do in real life: move your head closer and look.

The VR environment will offer the chance to see software in the context of an entire elections system, including polling place signage, virtual election officials, and virtual voters. This will allow both designers and stakeholders to see and understand the interaction among software, hardware, and humans and to ensure that a coherent experience is presented to voters.

Furthermore, the VR experience allows stakeholders, such as members of the disabled community, to provide feedback for incorporation into the final design. VR can also be used to simulate many disabilities, allowing anyone to experience voting under a variety of conditions (e.g., blindness, a wheelchair, deafness or decreased mobility).

## 1.8 Project Storytelling

Describing what makes STAR-Vote different and better in terms the average person can understand is a big challenge, and most people have a hard time placing trust in something they cannot understand. It is crucial that the story of STAR-Vote creates understanding and builds trust among those who will cast votes on it, as well as potential *STAR-Vote Entity* partners.

The STAR-Vote brand should be built from first principles with total disclosure, full exposure, and utter transparency. We must build trust in it by explaining what it does, and why it does it that way, from start to finish. It should not be merely technologically 'open' via open source software and transparent engineering and accounting, but also transparent with respect to the people working to make it happen, both at Free & Fair and Travis County, and their methodologies and processes.

We have several means by which to help tell the story of STAR-Vote, nearly all of which are part-and-parcel of how we develop high assurance systems today. For example, we commonly collaborate via distributed version control systems like Git, use collaborative development environments like GitHub, and use online live collaboration tools like Google Docs and Slack. All of these technologies have transparency as a built-in core feature, and they all facilitate sharing what the Free & Fair team is doing, not just with each other and Travis County, but with the world.

Likewise, in developing an assurance case about a product, one has to precisely document, in a traceable fashion, every aspect of a system and the decision-making that goes into its creation. This process results in a book—for this project, the STAR-Vote Book—readable by the expert, and approachable by the novice (if we keep that audience in mind), as we build our assurance case. Finally, as a normal part of how we operate we publish blog posts about things we learn as individuals and as a team and milestones we reach in our R&D.

We intend to continue to work in this fashion while performing on the STAR-Vote project for Travis County, and doing so will help tell the STAR-Vote story. Some other ideas about how we can help Travis County perform storytelling about STAR-Vote are included in Section 16.

In the RFP, you state:

*Vendors working on this project must agree to openness and full disclosure, and maintain a very high standard of ethics in fact and perception. It is imperative that a project of this size and sensitivity be conducted by vendors who are willing and able to withstand a high degree of scrutiny.*

This bold and unprecedented project calls for a bold and unprecedented team of actors offering unbridled transparency and documentation, and that is exactly what Free & Fair brings to the table. We intend to not merely satisfy, but far exceed, your demands for openness and full disclosure.

## 2 Part I, 1.0 General Requirements

All requirements of Part I are **acknowledged**, except as noted in this section.

### ***E.2.1 Developing a New Business Structure***

*Travis County (or a consortium of other STAR-Vote™ counties) must retain all intellectual property and proprietary rights in and to the STAR-Vote™ Elements B, C (only the custom software/firmware for existing hardware) and all legally protectable elements and components of it.*

**Acknowledged with objection.**

#### **Alternate Wording:**

Travis County (or a consortium of other STAR-Vote™ counties) must retain all intellectual property and proprietary rights in and to the STAR-Vote™ Elements B, C (only the custom software/firmware for existing hardware), and all legally protectable elements and components of it, with the exception of existing cryptographic libraries and software development frameworks. As the owners of the STAR-Vote system, Travis County will release STAR-Vote under an OSI approved license either within 6 months of IP transfer to Travis County or prior to Travis County assigning the IP of the system, whichever comes first.

In order to maintain a mutual interest in the STAR-Vote system, the Contractor will become a founding member of the entity created to manage the STAR-Vote system with voting rights commensurate with the voting rights of Travis County, and will be given a seat on the board of that entity.

#### **Implementation Approach:**

N/A

#### **Justification:**

Open Source software is core to Free & Fair's mission statement, as we believe it results in the strongest possible elections systems. Open Source systems are verifiable by the general public, offer flexibility for the jurisdictions that use them, and allow input from a wide range of technical sources. As such, we believe it is important for Travis County to commit to a timely release of the STAR-Vote system under an OSI approved license if IP is assigned to the County.

By ensuring that the Contractor is a founding member of the entity created to manage the STAR-Vote system, Travis County can both retain the IP and reap the benefits of Free & Fair's continued participation in the project. This approach will support the development of the healthy ecosystem of developers and users essential to support Travis County's vision of open source election technology managed by citizens and government. The Free & Fair team has a stellar reputation within the open source development community and will attract significant resources to the STAR-Vote project. Since so many jurisdictions across the United States are preparing to procure election technology in the near future, building momentum quickly for STAR-Vote will significantly improve the long-term prospects for a large, competitive, powerful community of developers and users.

**Cryptography.** Our proposed alternative cryptographic protocol (the “STAR-Vote Mix-Net Protocol”) depends on the Verificatum Mix-Net (VMN). The scope of what VMN offers is significant enough that to undertake a reimplementations would exceed the County’s initial development budget. We do not see any way around the use of VMN without massively inflating the price of developing the system. The intellectual property rights for this library are not owned by Free & Fair and cannot be transferred to Travis County.

However, the VMN is made broadly available via the Verificatum License 1.0, which allows clients to modify, use, and publish modified versions of the VMN.<sup>5</sup> The software is free for pure research purposes, so any modified versions developed by the research community can be used in the same way. Nominal license fees, proportional to use, must be paid for any modified version used for election purposes. As such, we have integrated these estimated license fees for VMN’s use in Travis County into our proposed development cost.

### 3 Part II, 2.0 Detailed Response: Project Management

#### 3.1 Project Team

The project team brings together internationally recognized technical and domain experts who are committed to improving democracy and its realization through e-government systems.

##### 3.1.1 *Joseph Kiniry, Project Manager*

- Lead the project and assume overall accountability for its success
- Set the technical direction for the project

##### 3.1.2 *Daniel Zimmerman, Chief Architect*

- Architect the STAR-Vote system and its components
- Develop the assurance case for the STAR-Vote system

##### 3.1.3 *David Cok, High-Assurance Software Specialist*

- Provide high-assurance development, validation, and verification of the STAR-Vote system
- Develop and manage the assurance toolchain for the STAR-Vote system

##### 3.1.4 *Joey Dodds, Rigorous Systems Engineer*

- Produce formal and informal system and component specifications
- Provide rigorous systems engineering

---

<sup>5</sup> The license is found at [http://www.verificatum.com/VERIFICATUM\\_LICENSE\\_1.0](http://www.verificatum.com/VERIFICATUM_LICENSE_1.0) and a comprehensive presentation of the rationale for the license is provided at [http://www.verificatum.com/html/rationale\\_for\\_license.html](http://www.verificatum.com/html/rationale_for_license.html).

### *3.1.5 Stephanie Singer, Project Coordinator*

- Lead internal coordination of project team
- Produce progress reports to Travis County
- Provide timely responses to questions and issues raised by Travis /County
- Participate in on-site visits
- Serve as primary point of contact for Travis County's Enterprise-wide System Project Manager to assist with coordinating integration of the Elements

### *3.1.6 Morgan Miller, UI/UX Lead*

- Incorporate User Centered Design in the discovery, design, and build stages of the project
- Perform usability and accessibility testing
- Coordinate and communicate with UI/UX subcontractors and between UI/UX team and engineering team
- Consult on usable security

### *3.1.7 Douglas Wikström, Cryptographer*

- Create and assess cryptographic protocol
- Serve as expert consultant on general elections cryptography matters

### *3.1.8 Michael Kiniry, Project Storyteller*

- Serve as communications professional and media liaison
- Perform as photographer and videographer for documentation and archival purposes
- Co-author and edit the STAR-Vote Book (subject to client need)
- Direct the STAR-Vote Short Films (subject to client need)

### *3.1.9 Drew Davies, User-Centric Design of Election Systems UI Expert*

- Provide concept, design, and iteration of prototypes of digital user interface (UI) elements (ballots, on-screen guides, administrative software modules, reports, etc.)
- Provide concept, design, and iteration of prototypes and final buildout of physical system elements (ballots, receipts, voter instructions, user manuals, etc.)
- Collaborate and consult regarding best practices in user-centered design, user experience (UX), and user flow through the entire voter experience
- Incorporate User Centered Design in the discovery, design, and build stages of the project
- Perform usability and accessibility testing
- Coordinate and communicate with UI/UX subcontractors and between UI/UX team and engineering team
- Consult on usable security

### 3.1.10 Industrial Design and System Prototyping

- Create industrial design of hardware components
- Test COTS components
- Provide hand sketches and CAD modeling
- Generate physical models and prototypes
- Test usability and reliability
- Supply and support Virtual Reality environment for testing and demonstration

### 3.1.11 Stefan Carpentier & Daniel Nelson, Hardware Systems Design and Engineering for Production

- Provide oversight of mechanical development
- Validate product architecture
- Create DFM studies to support easier, higher yield manufacturing
- Provide physical implementation of hardware that meets given industrial design specifications
- Generate design for storage, deployment, and security

### 3.1.12 Harri Hursti, Cryptography, Cybersecurity, Audits, and Assurance Case

- Consult on cryptographic security of system (theoretically and practically)
- Provide internal red team assessment of hardware security
- Consult on overall security of system
- Create manual for STAR-Vote audit administrator
- Provide audit training and facilitation
- Review assurance case structure and content for clarity and completeness

## 3.2 Project Management Practices

In this section, we review Free & Fair's project management practices. Our core project management principles focus on **Customer Caretaking**, **Social Contracts**, **Continuous Improvement**, **Artifacts and Evidence**, and **Transparency**.

**Customer Caretaking.** For all projects, we have a dedicated Free & Fair team member whose role is to represent the interests of the client. They are actively engaged with the client and have a role in all project management decisions. They build a deep trust relationship with the client's key performers. This position is a reflection of the trust relationship between us and our clients.

**Social Contracts.** Our systems engineering artifacts capture technical interdependencies among project team members, but the glue that holds the team together and makes the team work well is our collective social contracts. Our performers explicitly discuss and acknowledge client-supplier relationships between team members and always perform to exceed not only the expectations of our external client (e.g., Travis County), but also each internal client (another team member).



**Continuous Improvement.** Social contracts are renegotiated frequently and fluidly and are directly reflected upon immediately upon completion. For example, at the end of a thirty-minute stand-up meeting discussing a milestone that we just reached and what comes next, we often have a five-minute discussion about what worked well and where improvements can be made with regards to that particular piece of work. In particular, we focus on its embedded social contracts. The individuals in our organization always attempt to maximize efficiency, impact, and joy at work.

**Artifacts and Evidence.** We focus on artifacts and evidence in a project or product. “Meta” aspects like processes and checklists serve meaningful outcomes. This focus on the meaningful is pervasive. Principles trump rules. For example, provable security is mandatory; “security theater” is prohibited.

**Transparency.** Finally, whether it is with regard to our technology, business practices, or project management approach, transparency is the core principle by which we operate. Telling each other, and the client, when something is working well or working poorly, early and honestly, is common. If necessary, we will tell a client that a technical direction they are excited about is inappropriate and provide objective evidence to justify that conclusion. We always keep the client informed, whether we are ahead of the game or behind the eight ball. In all aspects, and for all projects, we believe that transparency is the keystone of our operation. Without it, our election systems cannot be trustworthy and will not be successful.

Now that we have provided an executive summary of our principles, we address the more detailed matters requested in the RFP.

### 3.3 Schedule, Milestones, and Deliverables

The implementation stages for Elements B and C differ, because Element B is primarily a software product while Element C is primarily a hardware product.

The stages for Element B, and our proposed schedule for carrying them out, are:

- Requirements Verification & Validation (RVV): Months 1–2
- System Design and Architecture (SDA): Months 1–4
- System Development (DEV): Months 1–17
- Functional and Technical Testing (FTT): Months 3–17
- System and Integration Testing (SIT): Months 16–18
- User Acceptance Testing (UAT): Months 16–18

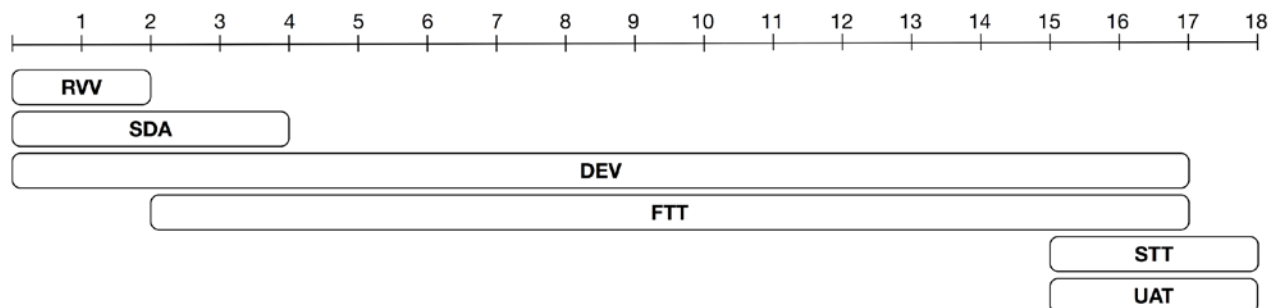


Figure 1: Element B Proposed Schedule

Table 1 shows the milestones and deliverables that occur during each stage of Element B development. We have included milestones for large, user-facing software modules, as well as for interim deliveries of system snapshots to the Element D Red Team and the completion of user manuals and instructional materials. User experience testing and functional/technical testing of each module will be complete when its milestone is reached.

Except where dependencies are explicitly indicated, development of each individual module of Element B is independent from development of the rest. The order in which the milestones and deliverables are listed in the table is, therefore, not the order in which they must be completed during project execution; we intend to determine the desired order of module completion during contract negotiations with Travis County.

Element B Milestones by Stage		Dependencies	Deliverables
<b>Requirements Verification and Validation (RVV)</b>			
B.1	Detailed Requirements	None	Outline of Detailed Requirements
<b>System Design and Architecture (SDA)</b>			
B.2	Architecture, Protocols, APIs, Data Formats	B.1	Architecture Documents, API and Data Format Descriptions
<b>System Development (DEV)/Functional and Technical Testing (FTT)</b>			
B.3	In-Person Ballot Assembly and Generation	B.2	In-Person Ballot Assembly and Generation Module
B.4	Ballot Control Station	B.2	Ballot Control Station Module
B.5	Voting Station	B.2	Voting Station Module
B.6	External Red Team Snapshot 1	B.2-B.5	
B.7	Tabulator	B.2	Tabulator Module
B.8	Sample Ballot and Web View	B.2	Sample Ballot and Web View Module
B.9	Trustee System	B.2	Trustee System Module
B.10	Risk Limiting Audit	B.2	Risk Limiting Audit Module
B.11	External Red Team Snapshot 2	B.7-B.10	
B.12	Audio Ballot Reader	B.2	Audio Ballot Reader Module
B.13	Public Tally Verifier	B.2	Public Tally Verifier Module
B.14	Bulletin Board	B.2	Bulletin Board Module
B.15	Open Source Reference Modules	B.2, B.13, B.14	Open Source Reference Modules
B.16	Manuals and Instructional Materials	B.2-B.15	Manuals and Instructional Materials
<b>System and Integration Testing (SIT)/User Acceptance Testing (UAT)</b>			
B.17	Module Testing and Integration	B.2-B.15	All Element B Modules

*Table 1: Element B Proposed Milestones & Deliverables by Stage*

The stages for Element C (explained in further detail in Section 5.8.2), and our proposed schedule for carrying them out, are:

- Scoping (SCP) Months 1–3
- Detailed Design (DES): Months 3–13
- Testing (TST): Months 8–15
- Production Ramp (PRR): Months 15–17
- Certification (CER): Months 15–17
- Release to Market (RTM): Month 18

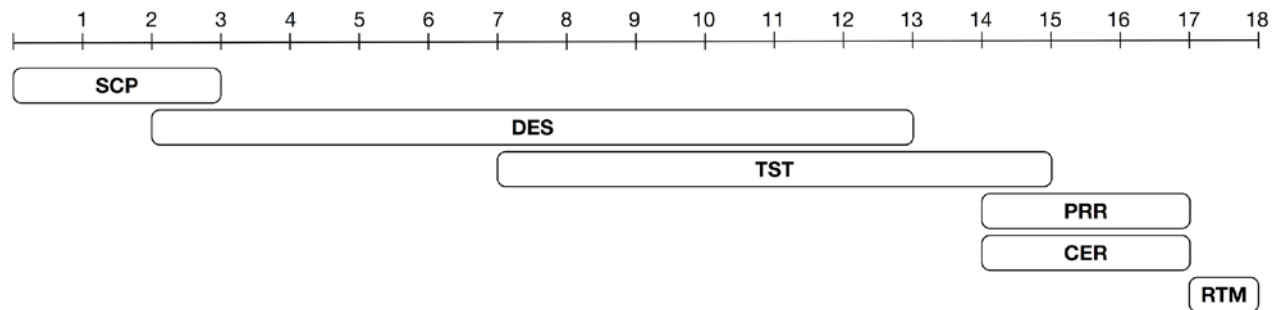


Figure 2: Element C Proposed Schedule

Table 2 shows the milestones and deliverables that occur during each stage of Element C development. We have included milestones for four design iterations, as well as certification and delivery of the production-ready design. The actual number of design iterations during the project will be determined jointly with Travis County.

Element C Milestones by Stage	Dependencies	Deliverables
<b>Scoping (SCP)</b>		
C.1 Mock-up Samples	None	Mock-up Samples
<b>Detailed Design (DES)</b>		
C.2 First Design Iteration	C.1	First Design Schematic
C.3 Second Design Iteration	C.2	Second Design Schematic
C.4 Interim Solution	B.2	Interim Solution
<b>Testing (TST)</b>		
C.5 Third Design Iteration	C.3	Third Design Schematic
C.6 Fourth Design Iteration	C.5	Fourth Design Schematic
<b>Production Ramp (PRR)/Certification (CER)</b>		
C.7 Certification	B.2, C.6	Certification Documents
<b>Release to Market (RTM)</b>		
C.8 Ready for Manufacturing	C.7	Final Design Schematic Ready for Production

Table 2: Element C Proposed Milestones & Deliverables by Stage

The only inter-element dependencies are that both the Interim Solution and the final product for Element C depend on the Protocols, APIs, and Data Formats of Element B.

### 3.4 On Time and Within Budget

We use a combination of strategies to ensure on-time, within-budget delivery. Our rigorous systems engineering methodology has been refined over the past fifteen years and incorporates the best elements of many “old” processes and methods (such as the waterfall and spiral processes, and several design methodologies including Fusion, OCL, and BON) as well as several “new” processes that repackage old ideas (such as “agile” processes). IT professionals will find some things familiar about our methodology, but some ideas, techniques, and technologies will be wholly unfamiliar at first. Each aspect of our methodology has been rigorously defined, refined, and used for years and much of it has been published in peer-reviewed papers in top academic forums. It is also highly cited in other contexts, such as the aforementioned NIST IR report for the White House.

We start by specifying the entire system design; as we build, we rigorously test each component, baking quality into every stage of the process and avoiding costs and delays typically associated with defects discovered after the fact. By formally specifying the initial design, and developing the implementation based on the resulting specification, we guarantee that we are implementing exactly the specified system. Quality assurance is achieved through strict configuration management and systematic validation of the code as well as through the evidence-based artifacts and documentation produced. In addition, we use continuous integration, a practice that is proven to improve efficiency and accuracy of system development. Finally, we use continuous deployment to allow all project participants, including Travis County staff, to test the latest working version of the software.

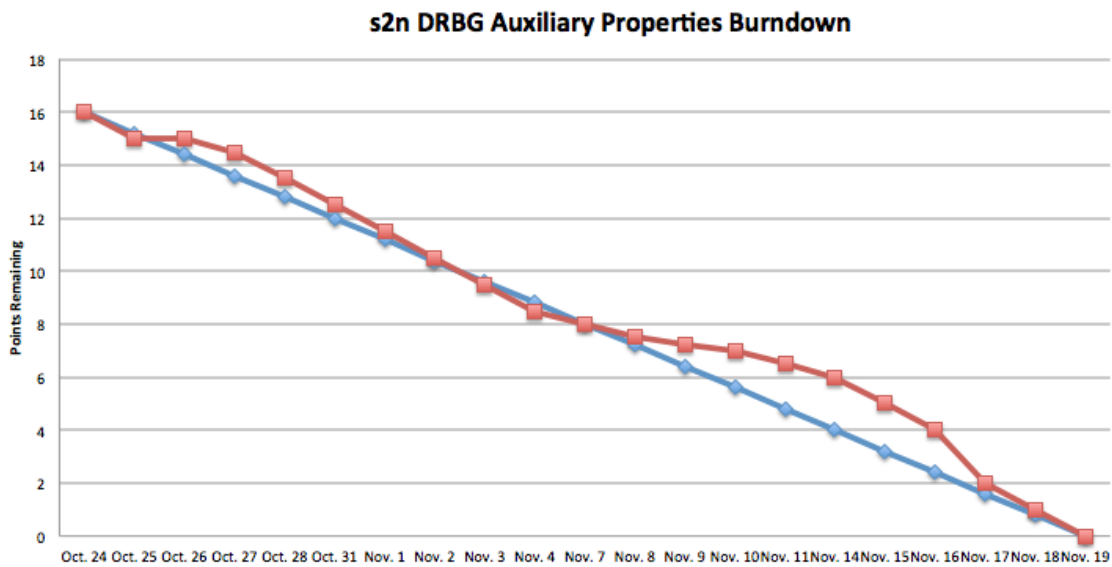
The milestones listed in Section 3.3 can be used to track the development of the system. At these points, we will provide evidence in the form of deliverables that development is on track.

In addition, once our more detailed design steps are completed, we keep a list of timed progress points with a granularity typically no finer than one point per week. From these points, we generate burndown charts, allowing for an accurate view of progress organized by the number of remaining points as time progresses. These burndown charts can be sent in a progress report, or they can be available for the County to view in real time.

Below we have attached an example burndown chart that we provided to Amazon to represent progress towards a milestone in our s2n verification work<sup>6</sup> referenced in the Qualifications Questionnaire. The red line represents our actual progress, and the blue line represents ideal progress. Since this work was a short-term project, we used daily progress points and sent weekly reports to the client. If the burndown chart showed we were behind schedule (meaning the red line was above the blue line), our weekly report contained an explanation for that delay as well as our plan for returning to schedule. We can provide similar burndown charts for any and all recent projects.

---

<sup>6</sup> <https://galois.com/blog/2016/09/verifying-s2n-hmac-with-saw/>



### 3.5 Test Methodologies

Testing provides some degree of assurance that a system will behave according to its requirements. In mainstream software engineering, test-driven development, often couched in agile processes, is in vogue and considered a best practice. While we realize testing is important, we do not use testing in the same fashion as other R&D organizations. We are different because, as discussed elsewhere at length, we use a rigorous systems engineering methodology based upon applied formal methods.

Essentially, because we reason about programs and their specifications, rather than hand-writing and hand-maintaining tests that only describe a small fraction of a system’s functionality, we formally describe what a system is meant to do and prove (formally, mathematically, mechanically) that the system will always behave that way under all conditions. These correctness proofs give as much assurance as testing every possible state the system can ever be in. This field of R&D is known as formal verification; many members of our team are world leaders in this topic, having been professors and professionals inventing and publishing new concepts, mathematics, tools, and techniques in this area for decades.

Many properties a system should have are, in fact, untestable. Security is one of the most noteworthy. Certainly, one can look for known bad practices or “gotchas”—what is often viewed as security testing in mainstream software engineering—but avoiding all of the known mistakes one can make says nothing about all of the possible unknown mistakes that can introduce security failures in systems.

As an example, it is impossible to test that the STAR-Vote end-to-end verifiable protocol is, in fact, secure. No security evidence exists for the protocol, and security cannot be guaranteed through testing. This means that a security proof is necessary. We will deliver such a proof as one of the outputs of our development process in this project. Likewise, showing that the STAR-Vote implementation actually implements exactly the STAR-Vote protocol—no more, no less—can only be formally verified, and cannot be achieved by testing. We are the premier

organization in the world on this topic, as our seventeen years of R&D for the federal government attests.

Despite the level of assurance we can achieve through formal verification, there is still much to be learned from executing a system and examining its behavior under execution, whether in a virtual environment (VR or virtualization) or in a physical one (across different CPUs, operating systems, etc.). Below we explain the means by which we test, and how that testing complements formal verification.

### 3.5.1 *Software Testing*

Free & Fair will ensure that the delivered Elements meet their intended security, performance, and accuracy (correctness) requirements by applying dynamic and static checking at multiple levels.

Dynamic checking (classic testing) is applied at three levels. The first is unit testing. At this level, each basic software component of a system is tested to ensure it meets its specification. The specification is obtained as part of the refinement of the high-level system requirements through the design process. Using our tools, most of these tests will be generated automatically. Unit tests provide a low-level indication that the basic components of a system are working as intended and provide an early warning if changes cause requirements and implementation to diverge. These will be performed under live conditions.

The second level of dynamic checking is functional testing—testing that the overall functionality of the system is correct (e.g., that it counts ballots correctly). For these tests a range of use scenarios is designed, with test scenarios including even unlikely combinations of input data. These tests are designed to cover the full requirements of the system. Our functional tests can be designed without a full implementation in hand, based on the system requirements and the input data formats; this will help ensure that the tests accurately represent the system requirements without being influenced by implementation choices. These will be performed under live conditions.

The third level of dynamic checking is user interface (UI) testing. UI testing is different, because it takes special tools to drive a UI for a system in a way that is repeatable but still at the level of a human user. There are two kinds of UI testing to consider. First, during UI design, a prototype of the final system is used to simulate the user's experience of the actual system. We will use this prototype to get early and regular feedback from users, both via interaction with the system in Virtual Reality and via prototypes (we discuss this in more detail below). This feedback will inform our iterative design improvements. Additionally, testing sessions can be observed, recorded, and shared with other team members to ensure that end user experience remains central during the design process. We will invite Travis County officials to both take part in and view these studies, either directly or remotely. This will give Travis County a deeper understanding of how the users of the system are driving our design choices. During the design process, these will be performed by live users on systems that are increasingly accurate mock-ups of the eventual technology. See Section 3.5.4 for further detail.

Second, there is testing to be sure that the implemented UI conforms to the design and the product requirements built into the design. This kind of testing is automated using tools that can drive the UI based on test scenarios; the testing is run regularly to be sure that no inadvertent



code changes cause the implementation to diverge from the design. Since formal methods for verifying UI functionality and responsiveness are less mature than for algorithmic verification, UI testing is an important component of the overall assurance case.

Dynamic checking only provides indicative evidence that a system performs as intended, because it is typically not possible to test all possible scenarios. With this in mind, we will not only report test success, but also indicate what fraction of system behaviors we cover using dynamic checking.

In addition to dynamic checking, Free & Fair will use static (formal) verification to prove that key components implement the system requirements. In static verification, implementation and specification are each translated into an equivalent logical representation and automated proof tools are used to ensure that the implementation satisfies the specification. These tests are performed directly on the software and do not have a physical component. This kind of verification is the formal variant of what is known by many names, such as component-based, component-level, subsystem-level testing. Because our specification and reasoning methods are compositional, these techniques also subsume what is normally known as integration testing. These formal checks are also automated and can be replayed regularly to be sure that requirements and implementation stay consistent as the project progresses. We discuss our rigorous systems engineering method in greater detail in Section 4.7.

### 3.5.2 *Hardware Design Testing*

Close cooperation with the end manufacturer makes the design process shorter, the transition to manufacturing easier, and the resulting design of very high quality and reliability. Free & Fair has decades of collective experience delivering reliable, high quality hardware. We will work closely with our selected manufacturing partner to define appropriate hardware engineering testing, general reliability testing, environmental resilience testing, materials durability, finish hardness, and fit and finish of parts. Some specific examples include resilience to drops from expected use heights, resistance to temperature and humidity ranges expected during use and storage, and survivability of transportation (using ASTM specifications designed to emulate transit modes). Standardized reliability testing for a variety of aspects assures this high-quality end product from the initial part exiting the manufacturing line to the end of the product's useful life. These tests are all performed under live conditions.

### 3.5.3 *Security Testing*

In addition to correctness, security is critical to election systems. Correctness guarantees state that, if used as anticipated, the system will give a correct result. Security guarantees state that, if the system is used in an unanticipated way, it *cannot* give misleading results. Assurance that nothing bad can happen cannot be provided by dynamic testing; it can only be provided by formal proof. Proofs of security guarantees will be among the assurance artifacts and arguments that Free & Fair produces in support of the delivered Elements. These tests are performed directly on the software and do not have a physical component.

### 3.5.4 Usability and Accessibility Testing

As User Centered Design (UCD) is incorporated through the discovery, design, and build stages of the project, usability testing is woven throughout system design and development.

Usability goals and assessments are grounded in a research phase at the beginning of the project during which current and relevant research, both academic and corporate, is explored, vetted, digested, and shared by the team. Our UCD lead will spearhead the research and create a findings report to share with the team at large, ensuring the group has a shared understanding of relevant previous work. The UCD lead will also act as a research liaison, helping guide other team members to personally relevant materials to support their roles in the project.

Since the audience must be broad and inclusive, our approach will be to focus on high-needs cases and adopt an agile, iterative approach with many rounds of lightweight user testing. During this phase, we will ensure the designs are Section 508 compliant.

Our designers will start with lightweight design iteration and incorporate user testing as early as possible. These early tests may be done with simple paper prototypes to test out ideas. As the ideas progress and refine, an interactive prototype is constructed. Our usability testing is purely focused on prototype development. Feedback and input provided by users shape the UI design concepts in the context of the stated product requirements.

**Overview of Usability and Accessibility Testing.** Early user testing will be done on a bi-weekly basis with 5 to 8 users recruited through professional networks. We take our testing approach from user experience experts in the Nielsen Norman Group, who wrote a seminal article on the ideal number of participants and structure of user testing sessions. They state that 5 to 8 participants yield almost all of the meaningful findings. Additionally, they suggest that teams interested in getting their design down to a very small margin of error run repeated smaller testing sessions instead of few larger testing sessions.

As the design matures, testing will continue and will culminate with formal audience definitions. Our team will run one more user testing session after the design process has finished. Feedback from the testing will be incorporated and a final design will be released.

As such, usability and accessibility testing takes place in several different phases of the project. UI prototypes witness usability testing during design, even before an interactive demonstration is complete. System prototypes witness usability testing in Virtual Reality prior to any hardware being built. Interactive prototypes are created for all UI components. Since UI specifications and prototypes are a part of the static and dynamic specification of the productized implementation of UI subsystems, once those subsystems are completed and have a complete assurance case, they will not need usability or accessibility testing prior to being submitted for certification at our VSTL.

Observational research is collected throughout these studies and will be integrated across the team (and potentially with the performer on Element E) to include accessibility and inclusivity of all users identified throughout the up-front planning and profiling of users. Our design team uses a variety of methods including storyboarding, concept testing, heuristic review, journey mapping, and user frameworks for testing and validating concepts. Low-fidelity prototyping, usability studies, and user interviews provide iterative feedback that is incorporated into concepts that are fully baked and provided as final design that meet the objectives of the County, as

detailed in the RFP and the earlier RFI. Usability testing can be applied to many facets of product development from the early stages of research through the final product launch.

**Details of Accessibility Testing.** Our team intends to do regular user testing to benefit from iteration both for designers and for test participants. Assuming the research and design phases last approximately four months, we will test approximately six times on roughly a bi-weekly basis.

<b>Test 1: Paper prototype of early concepts</b>	
<i>Equipment</i>	Paper and pencils. A quiet testing room for in an in-person study.
<i>Number of participants</i>	5–8
<i>Profiles</i>	Ad-hoc basis drawn from a personal network. Effort will be made to target diversity around gender, age, race, education level, and familiarity with computer technology.
<i>Purpose</i>	Iterate quickly and identify immediate problems.
<b>Test 2: Paper prototype</b>	
<i>Equipment</i>	Paper and pencils. A quiet testing room for in an in-person study.
<i>Number of participants</i>	5–8
<i>Profiles</i>	Ad-hoc basis drawn from a personal network. Effort will be made to target diversity around gender, age, race, education level, and familiarity with computer technology.
<i>Purpose</i>	Iterate quickly and identify immediate problems.
<b>Test 3: Low fidelity digital prototype</b>	
<i>Equipment</i>	Computers, one for each test participant. A quiet testing room for an in-person study.
<i>Number of participants</i>	5–8
<i>Profiles</i>	Ad-hoc basis drawn from a personal network. Effort will be made to target diversity around gender, age, race, education level, and familiarity with computer technology.
<b>Test 4: Medium fidelity digital prototype</b>	
<i>Equipment</i>	Remote testing with computers supplied by participants at home. A prototype will be published online, allowing for remote testing. Screensharing software will be used to capture video of participants engaging with the system and narrating their experience and expectations.
<i>Number of participants</i>	5–8
<i>Profiles</i>	Ad-hoc basis drawn from a personal network. Effort will be made to target diversity around gender, age, race, education level, and familiarity with computer technology.

<b>Test 5: High fidelity digital prototype built</b>	
<i>Equipment</i>	Remote testing with computers supplied by participants at home. A prototype will be published online, allowing for remote testing. Screensharing software will be used to capture video of participants engaging with the system and narrating their experience and expectations.
<i>Number of participants</i>	5–8
<i>Profiles</i>	Formal screening and identification of users based on research and prior testing results. Target users will be identified through the research and early design processes.
<b>Test 6: High fidelity digital prototype</b>	
<i>Equipment</i>	In-person users will visit a lab environment mimicking a polling place set up by our team. Session moderators will provide an introduction to the system but after the user has begun the voting process the moderators will not be permitted to help. Additional testing observers will watch remotely. The system will record the screen as the user progresses through.
<i>Number of participants</i>	100 as required in the VCIF
<i>Profiles</i>	Formal screening and identification of users based on research and prior testing results. User demographics will be age, race, education level, and gender.

### 3.5.5 Final System Testing

The final type of testing is the testing of the hardware/software combination as it would be delivered. For this purpose, a set of *acceptance tests* is designed in cooperation with the client. The acceptance tests are made as automated as possible, but may also include manual tests. These tests are performed live.

One part of the regular reporting during the project will be the status of test suite development and test suite success, across all of the kinds of dynamic and static tests described above.

A final aspect of both dynamic and static checking is regular rerunning of tests. Typically test suites are executed (and static checks are re-run) every night and on every merge of new or corrected functionality into the release branch of software development. This is standard development practice and minimizes problems that can occur during component integration. It is also part of the continuous integration practice that is described in Section 4.8.

### 3.5.6 Product Certification

The finished design will be tested for compliance with FCC Class B standards for use in a residential environment as defined by CFR 47, Part 15. As well, though technically optional, the product will be UL listed to demonstrate best engineering practices with regard to product safety. The design will also be carefully reviewed to ensure compliance with accessibility guidelines, over and above what is strictly required by the ADA, and will conform to all applicable requirements of the Voluntary Voting System Guidelines.

### 3.6 Status Reporting

We are flexible with respect to status reporting frequency and format, which we typically negotiate with our clients before beginning work on a project. With most of our existing clients, we hold weekly or bi-weekly status meetings with the project team and the steering committee, and deliver formal status reports each month. A typical status report covers

- work accomplished in the past reporting period;
- work planned for the upcoming reporting period;
- project budget, spend, backlog, and other financial information;
- status of deliverables and milestones;
- project risks, issues, and action items;
- schedule and resource tracking against the project plan;
- performance metrics as agreed with the client; and
- questions or issues needing resolution by the client.

Travis County, any other STAR-Vote development vendors, and any Red Teams performing on Element D can have direct access to our development repositories and continuous integration dashboards. Thus, up-to-date status information with respect to module implementation progress and automated testing results will be continuously available to all concerned parties, who can review our high-level design or inspect our code at any level of detail they wish.

### 3.7 Change Management

Scope and change management is essential to project success. As part of our project management approach, we will perform the following actions:

1. Establish the initial Statement of Work (SOW) from the RFP with requirements classified in clusters (such as business, functional, technical and system requirements).
2. Establish a core user/subject matter expert group (subject to Travis County approval) with a comprehensive stakeholder representation at project start that owns requirements and related decisions.
3. Establish a change control body, including representatives from both Travis County and the Project Team.
4. Using the SOW, conduct a requirements verification and validation with the core user group as the first phase of the project to establish a baseline software requirements specification (SRS).
5. Establish a requirements traceability matrix (RTM) with the final set of verified requirements.
6. Develop a system corresponding to the RTM and establish traceability of the software to the requirements and the testing deliverables. Our development methodology inherently provides such traceability through the artifacts it produces.

On an ongoing basis, the County Liaison receives any requests for requirement changes from the various stakeholders. The items are passed through the change control process as follows:

1. New/changed requirements are first verified as being relevant and of priority by the core user/subject matter expert group.
2. A change request that outlines the impact of the change on staffing, time and cost is prepared by the County Liaison.
3. This request is provided to the change control body on the project, which makes a decision on whether, when and how the requirement should be met.
4. A change order is then either approved, clearly establishing the path of implementing the change, or denied, resulting in no change.
5. If a change order is approved, the project plan, SRS, RTM, and other relevant project documents are updated to incorporate it.

This process is facilitated by technology; in particular, change requests and actions are captured, discussed, traced, decided upon, and executed via email, regular scheduled meetings and an issue tracking system (or similar). Records are kept of all such interactions to facilitate traceability of changes.

### 3.8 Support, Maintenance and Upgrades

#### 3.8.1 Support

We propose an annual contract with a Service Level Agreement (SLA) for technical support for Travis County staff using the system.

#### 3.8.2 Maintenance

The only maintenance contract needed would be for non-COTS custom hardware components in Element C. Note that because the hardware specifications are open source, this maintenance contract can be bid competitively.

In the event of a software defect—unlikely because of the high assurance development techniques—Free & Fair will fix the defect at no charge to Travis County. In the event of hardware defects, any COTS parts can be easily replaced. Or Travis County may wish to obtain a service plan from their COTS hardware vendor(s).

If Travis County desires to enter into a maintenance contract with Free & Fair, our annual maintenance costs are 5% of purchase price for hardware and 10% of purchase price for software. “Purchase price” is the price at which we would sell the software to a jurisdiction, which for a system like STAR-Vote would be \$3.00 per citizen. For the maintenance cost estimates provided in Attachment 11, we assumed a population of 1.2 million for Travis County.

No upgrade contract is required. Free & Fair will not require Travis County to upgrade the software to maintain the functionality provided as part of this procurement. Any necessary work to package and install future versions, should Travis County elect to upgrade, can be included in the annual SLA contract with Free & Fair.

In the event that Travis County requires specific software upgrades (e.g., to comply with changes in election law), the County can reasonably choose to solicit bids for each particular upgrade



project. Open source software allows a variety of vendors to compete for upgrade work, so no single vendor can depend on proprietary lock-in.

Because Free & Fair proposes software designed to work on any operating system, operating system upgrades and security patches should not adversely impact the software. In the unlikely event that the software is adversely affected by an operating system patch or upgrade, the County can reasonably choose to solicit bids for each particular upgrade project.

## **4 Part II, 5.0 Detailed Response: Element B**

We propose to develop a set of open source modules to fulfill the requirements for Element B: In-Person Voting/Tabulation and Support Modules. We expect development to be expedited because of our prior experience developing artifacts that fulfill significant parts of the requirements, including a full demonstration version of the STAR-Vote system.

Our responses to the RFP's detailed questions about Element B are as follows:

### **4.1 5.1 Propose a file specification for an Election Definition import file and a preferred interface for importing data from a third-party system.**

Element B can be designed to use any file specification, as long as that specification is open and has an associated specification language.

We can use any standard interface for importing data from a third-party system as long as the third-party data is in an open format with an associated specification language. Two examples of such open formats are JSON (with JSON schemas) and serialized Google Protocol Buffers. Assuming that Element B is running on hardware substantially similar to our hardware recommendations, our preferred interface would be to import data from files on an SD card. If the third-party system cannot output such formats directly, we can create either a standalone application or a file translator module, integrated with the election definition import system, to parse the third-party output and translate it to an open format.

### **4.2 5.2 Propose a file specification for a Tabulator export file and a preferred interface for exporting the data to third-party systems into the Results Aggregation utility.**

Element B can be designed to use any file specification, as long as that specification is open and has an associated specification language.

We can use any standard interface for exporting data to a third-party system as long as the third-party data is in an open format with an associated specification language. Two examples of such open formats are JSON (with JSON schemas) and serialized Google Protocol Buffers. Assuming that Element B is running on hardware substantially similar to our hardware recommendations, our preferred interface would be to export data to files on an SD card. If the third-party system cannot read such formats directly, we can create either a standalone application or a file translator module, integrated with the tabulator export system, to translate our output from its open format to the third-party system's format.

- 4.3 5.2 (cont.) To simplify the design, development and testing of Element B, the RFP is requesting successful proposers to choose and propose specific COTS hardware to satisfy the requirements for the various hardware components identified in the RFP. Identify the selected COTS hardware computing platform(s) and devices for all functions within Element B, justify the selections, name the manufacturer, model and the process for quantity acquisition.

#### 4.3.1 General Considerations

The RFP calls for equipment that has the feel of a technology familiar to most people, such as a tablet. However, we believe that the tablets currently available on the market are not well suited for STAR-Vote. Until the market provides an appropriate COTS tablet, we recommend a small computer paired with a touchscreen monitor. Our recommended “tablet style” setup retains the ease of use and familiar touch-based interface that voters have come to expect from the tablets and mobile phones they use every day, but has the following advantages over currently available COTS tablets:

- Screen size that conforms to VVSG 1.1 requirements
- Enough available ports for required STAR-Vote elements
- Ease of lockdown
- Less manufacturer lock-in
- Choice of operating system
- Ease of maintenance/update

We describe these advantages in detail in the following paragraphs.

**Screen size:** VVSG 1.1 recommends a screen that is over 15 inches diagonal. There are very few tablets that meet this requirement on the market today. While we believe that an accessible interface is possible on a smaller screen, primarily because pixel densities have increased dramatically since the VVSG requirements were written, a larger screen still has accessibility benefits.

**More available ports:** Tablets typically have limited ports for interfacing with external devices. A voting station for STAR-Vote needs

- Ethernet for wired networking;
- At least 2 USB ports, one for the printer and one for an accessibility device;
- An audio jack for audio ballot reading.

None of the top tablets currently come with an Ethernet port, meaning that a USB port would need to be used with an adapter in order to provide a wired network connection. On many tablets, this alone will consume the single usable port; thus, the voting station would require a powered USB hub, which introduces more wiring, adds potential reliability issues, and requires an additional power supply.

On the other hand, our suggested system has a built-in Ethernet port and enough USB and audio ports to meet all foreseeable needs.

**Ease of lockdown:** Tablets present a security challenge because of the proximity of the power button and ports to the screen. Subtle industrial design is necessary for an enclosure that allows the touch screen to be used while both generally blocking access to the ports and buttons available on the outside of the tablet and allowing poll workers to use a port for accessibility devices upon request. With a small computer, on the other hand, limiting access to ports and buttons is as simple as locking the computer inside a box that is wired for exactly the ports and buttons that need to be exposed.

**Less manufacturer lock-in:** The complexity of design needed to enclose a tablet will almost certainly result in an enclosure that is designed and built specifically for a particular model of tablet. In order to change manufacturers, or in some cases even to upgrade to a new version of the tablet, it is possible that a new enclosure will be necessary. A simpler design incorporating an enclosure for a small computer and a standard VESA mount system for a separate touch screen display accommodates any computer and display of similar sizes.

**Choice of operating system:** The bootloaders of most off-the-shelf tablets are resistant to installing an operating system of the user's choice. Moreover, even if this were not the case, the hardware devices integrated into most tablets are only supported by the operating systems they ship with. For example, if you purchase an Android tablet, it is generally not possible to later install Windows on that tablet and retain full hardware functionality. With a small computer, it is possible to install the operating system of your choice and change it as necessary going forward.

**Ease of maintenance/update:** Many tablet failures require a complete replacement of the tablet. In the event of a disk, memory, or battery failure, the only recourse is a full replacement (or, in some cases, an extremely difficult repair). This can be time consuming and expensive.

With a small computer, on the other hand, any of those individual failures can be fixed by a plug-and-play replacement simple enough to be performed by poll workers during an election. The fact that the internal disk – typically, a small solid-state drive – is removable also has a number of other benefits. For example, all sensitive information and software lives only on the disk; if there is a very high security requirement for sensitive data, these small drives can be stored separately from the larger components, which will no longer need high security storage. Because the drives contain all of the software needed to run the in-person voting stations, software updates will not affect the computers and touchscreen displays used for voting.

#### *4.3.2 Specific COTS Hardware Recommendations*

The process of COTS design will include stress testing of COTS products. This testing may lead to changes in our recommendations for hardware makes and models. It will be in the interest of Travis County to allow some changes to the following specific recommendations. With the caveat that we recommend Travis County remain flexible on this score, our specific hardware recommendations at this time for Element B are the following.

##### **Ballot Control Station:**

- Intel NUC Mini PC, model NUC7i5BNK (or similar), equipped with 8GB RAM and a 256GB solid state disk
- ASUS 19.5” Touchscreen Monitor, model VT207N
- Brother TD-2120N thermal receipt printer with optional battery pack

- Uninterruptible Power Supply (UPS), either standalone or integrated into station furniture/*STAR-Vote Enclosure*

**Voting Station:**

- Intel NUC Mini PC, model NUC7i5BNK (or similar), equipped with 8GB RAM and a 256GB solid state disk
- ASUS 19.5" Touchscreen Monitor, model VT207N
- Brother PocketJet 7 thermal printer with optional battery pack
- UPS, either standalone or integrated into station furniture/*STAR-Vote Enclosure*

**Audio Ballot Reader:**

- Small Android Tablet (e.g., Samsung Galaxy Tab A) with a camera and a headphone jack
- Mounting device to secure tablet a sufficient distance from the voter to perform optical character recognition on a ballot placed in its camera's field of view

**Networking and Cabling:**

- Ethernet switches as appropriate for polling place size. We recommend the TP-Link TL-SG1048 48-port switch, which should be large enough for any polling place. This will provide an upper bound on the price of supplying all polling places with network hardware. In reality, many smaller polling places will be able to use smaller Ethernet switches.
- Category 6 network cables for ballot control stations and voting stations, and for connections between Ethernet switches as necessary. Ideally, cables will be custom cut per polling place to avoid waste.
- Standalone UPS for Ethernet switches

For both the Ballot Control Station and Voting Station we recommend deploying, and intend to design, a custom enclosure called the *STAR-Vote Enclosure* (described in Section 4.3.4). This enhances both security—by preventing access to unused expansion ports, inadvertent power cycling of the device by voters, etc.—and ease of setup by poll workers.

**4.3.3 Justifications for Specific Recommendations**

Our reasons for choosing Intel NUC computers include Intel's history of supporting their processors and computers, their build quality and reliability, and their past projected product roadmap. Since debuting the NUC line in late 2012, Intel has refreshed the line at least once, and sometimes twice, a year; the current NUC, recommended above, is a 7th generation model. Their development roadmap for NUC computers shows a similar refresh rate through 2018, and it is reasonable to expect them to continue development beyond then. In addition, several other companies manufacture Intel-based computers in similar form factors. This means that regardless of device lifespan, which we expect to be at least 5 years, it is very likely that new computing hardware meeting the STAR-Vote requirements will always be available.

Additionally, despite suggesting Intel NUC computers, all of our software will be hardware independent to allow different counties to make different purchasing decisions. That means that there is no requirement to make further purchases from Intel unless their hardware has proven

satisfactory in live elections and they have a quality replacement on the market at the time of purchase. Since the manufacturer specifications of COTS computing hardware are constantly changing, it is completely possible that we would recommend a different manufacturer when we suggest hardware replacement in order to save the purchasing county money.

We chose the ASUS VT207N display because it is lightweight, meets the STAR-Vote interaction requirements with its 10-point capacitive multi-touch system, and is large enough and has high enough resolution to meet all VVSG requirements. ASUS has a long history of producing reliable, high-quality displays, offers comprehensive warranty coverage for 3 years, and is committed to providing additional warranty and replacement parts for their EPEAT-certified products, such as the EPEAT Gold certified VT207N, for 5 years after the end of production. Given the evolution of the touchscreen display market, and the fact that our planned *STAR-Vote enclosures* support standard VESA mounting hardware for displays, there will likely be no difficulty obtaining suitable replacement display hardware when necessary.

For the Audio Ballot Reader, we envision a small tablet attached to a voting station or an independent station away from the voting stations with either a custom or COTS mounting device, such that its camera is capable of capturing an image of a ballot and performing optical character recognition (OCR) on it. This should provide sufficient accessibility for a vision-impaired individual to use the ballot reader. We chose Samsung's Galaxy Tab A because of its combination of price and performance, and Samsung's history of tablet reliability. A wide variety of tablets, and even cellular phones—ranging from budget Android devices to the most expensive Tablet PCs and iPads—could easily perform the functions required of the Audio Ballot Reader, and there will certainly be no difficulty obtaining alternative devices when replacements are necessary.

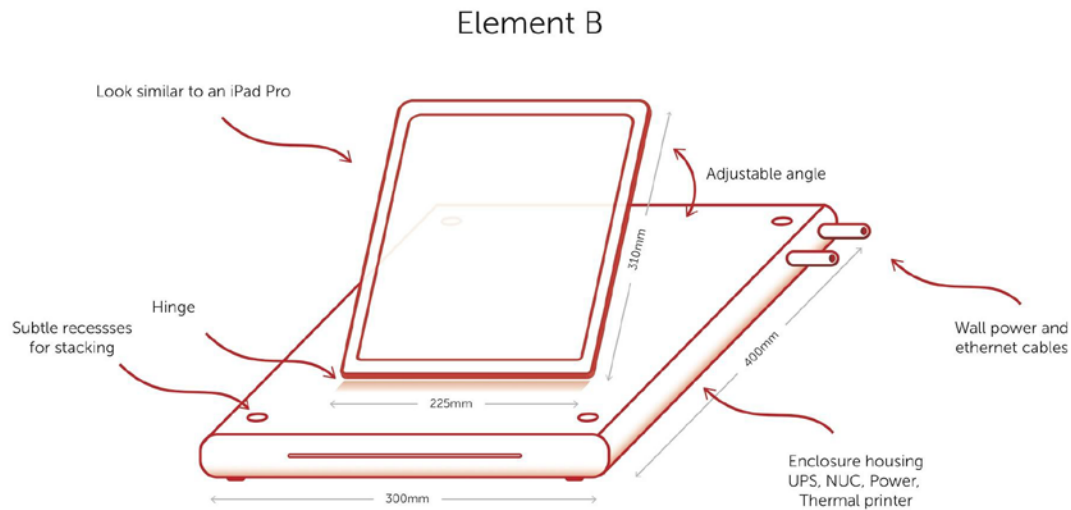
We have recommended quality network components that will meet the needs of Travis County. However, we are concerned that wired networks present too much of a purchasing and setup challenge to make up for any added security they have over wireless networks. We will help Travis County select a network solution that meets all of their needs.

#### 4.3.4 Industrial Design Necessary for In-Person Voting/Tabulation System

While it is entirely possible to build a functional in-person voting/tabulation system by purchasing the set of COTS components we have described and simply plugging them together on a desk, such a bare-bones solution will not fulfill the needs of voters, especially those with accessibility challenges. Moreover, there is much to be learned from parallel design efforts, such as we have witnessed in L.A. County, and the anti-patterns in design exemplified by existing vendors' products.

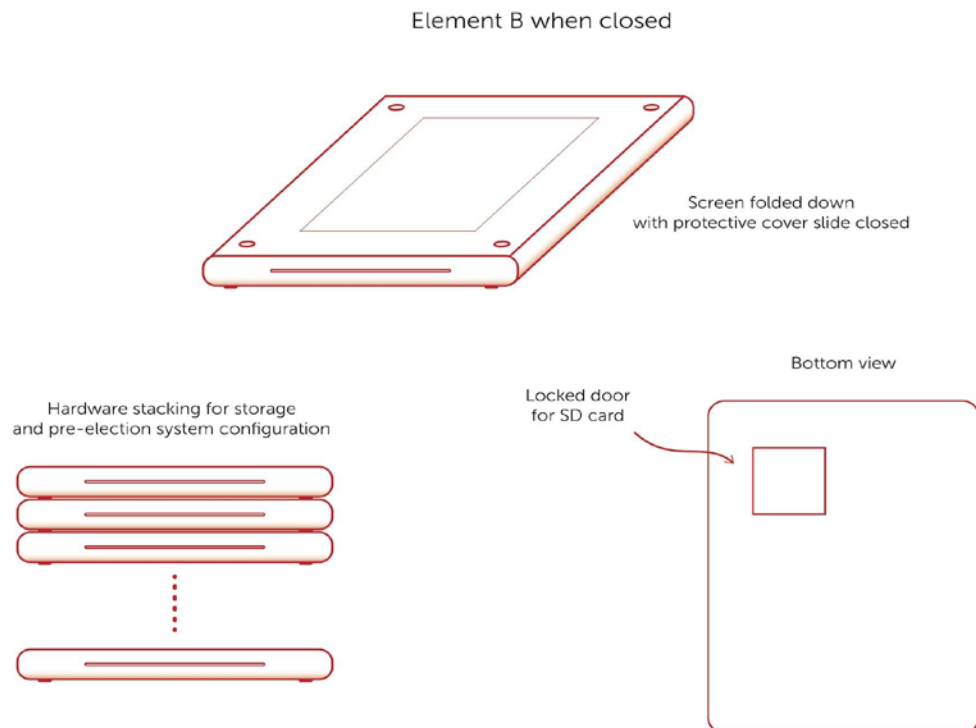
We are convinced that professional industrial design and prototyping is necessary to create a quality, COTS-based STAR-Vote in-person voting/tabulation system for Travis County. To execute on such a vision would require the participation of a high-end industrial design and prototyping firm, which unfortunately is well beyond the budget that Travis County has allocated to kick-start the development of the STAR-Vote system. We include two illustrations below of what a high-quality design for Element B might look like were we to have the resources to do a proper industrial design and prototyping effort.

Figure 4 shows an integrated In-Person Voting Station. Note the integrated hinged touchscreen, the secure enclosure (discussed below) housing all of the internal COTS components, and the paper feed slot on the front where the ballot and receipt emerge.



*Figure 4: Integrated In-Person Voting Station*

Figure 5 shows what the In-Person Voting Station might look like when in its storage configuration. Note that the enclosures fold completely flat for stacking and access to internal storage is via a digitally locked door on the bottom of the unit.



*Figure 5: In-Person Voting Station when in Storage Configuration*



We suggest that the overall goal of such a design project would be to create a bespoke *STAR-Vote Enclosure* that will be COTS by the end of the project. As such, the open hardware design of the *STAR-Vote Enclosure* will mean that any election official can order thousands of units (empty or fully configured) from a hardware manufacturing firm, achieving a cost savings as STAR-Vote deployments scale. In support of this effort, our team will develop a Virtual Reality (VR) environment of the system early in the design phase to get continuous feedback from our team and customer stakeholders to ensure an optimal design. We provide details about the Industrial Design and Prototyping process above and in Section 13, RFP Appendix F: Hardware Requirements.

The *STAR-Vote Enclosure* would be a custom computer case that is specifically designed for a supervised voting experience using the STAR-Vote end-to-end verifiable voting protocol. The *STAR-Vote Enclosure* would:

- securely house the aforementioned COTS hardware subcomponents,
- protect all exposed physical interfaces to COTS subcomponents,
- only expose exactly those interfaces necessary to fulfill the operational and non-operational (primarily security) requirements of the STAR-Vote in-person voting/tabulation system,
- have physical security superior to that of existing voting systems (e.g., poor physical locking mechanisms, security seals-based security theater, etc.),
- be designed for usability and accessibility, particularly taking into account the challenges of sight disabled, physically disabled, and wheelchair-bound voters, and
- have a polished look-and-feel that matches election officials' and voters' expectations with regard to fit and finish of quality hardware.

#### 4.3.5 Quantity Acquisition

Quantity acquisition would be carried out by working directly with the sales teams for each individual piece of hardware that would be purchased for the system. We would be sure to take advantage of all government and quantity discounts available. Furthermore, we would make the invoices for the hardware available; the cost of the hardware to Travis County will be exactly those invoice prices, plus any expenses we incur in provisioning and reshipping the hardware if we perform such tasks, with no additional mark-up. Finally, for the *STAR-Vote Enclosure*, we would establish a production pipeline with a hardware manufacturing firm for volume manufacturing and quantity acquisition.

#### 4.4 5.4 Provide a written preliminary hardware upgrade plan that projects selected COTS hardware computer platform(s) end-of-life and outlines alternate or new make and model for hardware replacement.

Note that the specific hardware recommendations here are preliminary. The design and testing phases of the project may lead to alternative recommendations.

We recommend that all components be sourced directly from their manufacturers, in order to take advantage of available bulk/government discounts.

Hardware Item	Expected Lifespan	Replacement	Alternate Make/Model
---------------	-------------------	-------------	----------------------

Hardware Item	Expected Lifespan	Replacement	Alternate Make/Model
Brother TD-2120N Thermal Printer with battery pack	10 yrs	Widely available	Epson Mobilink P60-II
Intel NUC Mini PC model NUC6i5SYK	5 yrs	Similar or upgraded model	ASUS VivoMini
ASUS 19.5" Touchscreen, model VT207N	10 yrs	Widely available	Dell S2240T
Brother PocketJet 7 Thermal Printer with battery pack	10 yrs	Similar or upgraded model	Printek Interceptor 800
CyberPower EC850LCD UPS	3 yrs	Widely available	APS BE850M2
Samsung Galaxy Tab A	5 yrs	Widely available	ASUS Zenpad S 8.0
ABR Mounting Device	30 yrs	Easily fabricated	n/a
AmazonBasics Lightweight On-Ear Headphones	10 yrs	Widely Available	Panasonic On-Ear Stereo Headphones RP-HT21
STAR-Vote Enclosure	30 yrs	Meant to be available from multiple manufacturers once hardware specs are publicly released	ArmorActive Gravity Flip Pro 2.0 VESA Table Stand
TP-Link TL-SG1048 48 port router	10 yrs+	Widely Available	Cisco SF200-48 SLM248GT-NA
Cables and connectors	10 yrs+	Widely available at about \$0.10/foot	n/a

Table 3: Hardware Recommendations

**4.5 5.5 The successful Proposer for Element B is required to work with the Red Team from Element D. Provide an outline of a plan for working with the Red Team.**

The Element D Red Team will have full access to our source code, and will not be limited to “black box” interactions with the system. They will have full access to our development repositories, and will be able to submit reports to us directly via a bug tracking service. This will allow interested parties to follow any discoveries made by the Red Team and see what action has been taken on any individual issue, as well as to check whether any issues have been resolved.

In addition, we have planned multiple internal releases to the Red Team for in-depth testing and analysis.

If any issue reported by the Red Team does not come associated with code to exercise the issue, we will create that code; thus, when each issue is fixed, we will be able to point to a specific revision of the software that contains visible evidence that the issue has been fixed. Continuing to maintain such examples will also ensure that further modifications to the software don’t reintroduce any issues discovered by the Red Team.

If desired, the Red Team can also interact with us directly during and after system development via multiple collaboration mechanisms (telephone, email, instant messaging, and videoconferencing).

- 4.6 5.6 Describe the various technologies proposed to be used during any development, including: programming language(s)/software libraries; test frameworks; algorithms (where these aspects are unusual or important to the design, including the selected cryptographic algorithms); and software backend for web-services and any implied hosting requirements. Reference items from Appendix D where possible.

Free & Fair has expertise in an extensive set of programming languages, libraries, test frameworks, algorithm and protocol design and analysis, distributed systems, software services, formal methods, and more. The nature of a given project or product, combined with any client constraints, informs the advice we give about choice in technology foundations.

The STAR-Vote RFP stipulates no explicit technology constraints other than the fact that the system must run on mainstream operating systems and on COTS hardware. Implicitly, however, there are multiple constraints.

First and foremost, there are assurance and security goals to consider. The STAR-Vote system is meant to operate properly in the presence of adversaries, both internal and external, with considerable skills and resources. As such, many mainstream technologies are wholly inappropriate for use in creating a STAR-Vote system. Programming languages and computational platforms specifically designed for high assurance systems are the right choice for STAR-Vote.

Second, If Travis County wants to foster a community of STAR-Vote providers, there are social-technological matters to consider. Travis County has an ambitious agenda to create an open source community around STAR-Vote, and hopes to see its adoption well beyond Texas. Consequently, while certain technology choices may be appropriate given the technical goals of the County, the use of esoteric technologies for the bulk of the development work would run counter to community-building.

Finally, there is the cost constraint, which rules out use of expensive commercial high-assurance technology, such as the operating systems used in systems we build for the Department of Defense. Also, **given the time and budget constraints of the STAR-Vote project, it is not possible to create high-assurance STAR-Vote software in C or C++.**

Consequently, in what follows we summarize the technologies that we believe are useful, affordable and relevant to the mission of Travis County and the STAR-Vote system. We realize, however, that during project execution—and perhaps even contract negotiations—we may make joint decisions with Travis County to use good and moderately popular technologies instead of great and esoteric ones. We are pragmatic in this regard, and promise to ensure that Travis County project personnel deeply understand the ramifications (to complexity, timeline, budget, and more) of making these kinds of technical decisions.

We have budgeted our proposal costs to be able to accommodate joint technological decision making, especially with regard to matters of programming language and platform.

#### 4.6.1 *Programming Languages*

While many companies make decisions about programming languages based upon institutional memory and momentum (i.e., staff only knows one language), at Free & Fair we have expertise in every mainstream and high assurance programming language in the world. As such, we make rational decisions based upon client requirements about which language to recommend and use. We advocate against the use of C and C++.

Unless further discussions with Travis County during contracting and performance reveal advantages of other choices, we propose to use some subset of the following languages and platforms. We choose this specific set of technologies because their capabilities, licenses, approachability, and quality meet or exceed the expectations of the County.

**High level programming and specification:**

- Dafny on .NET Core (the cross-platform implementation of Microsoft's .NET runtime)
- Scala & Java and the Java Modeling Language (JML) on the Java Virtual Machine
- Haskell
- Eiffel

**Low level native code programming:**

- SPARK
- Rust

**Mobile programming:**

- Java for Android
- Swift for iOS

**Other Formal Specification:**

- Cryptol and SAWscript for cryptographic algorithms
- F\* and Tamarin Prover for cryptographic protocols
- EBON/GSSL for system and architecture specification

**4.6.2 Software Libraries**

The set of core libraries applicable to STAR-Vote focuses primarily on cryptography, testing, and user interface development. The choice of cryptography libraries depends on programming language and licensing choices. Unless further discussions with Travis County during contracting and performance reveal advantages of other choices, we propose:

- Cryptography: BouncyCastle, Sodium, and Verificatum Mix-Net.
- User Interface: Qt, V-Play

#### 4.6.3 Test Frameworks

The choice of testing frameworks for validation of the STAR-Vote system depends on the programming languages used. Unless further discussions with Travis County during contracting and performance reveal advantages of other choices, we propose the following:

- Microsoft Unit Test and FsCheck, including the use of PEX, for .NET; JUnit, TestNG, and QuickCheck, including the use of JMLUnitNG, for Java
- Quickcheck and SmartCheck for Haskell
- EiffelUnit and ESPEC for Eiffel; QuickCheck for Rust
- afl and libFuzzer for fuzzing APIs

#### 4.6.4 Cryptographic Algorithms

Our cryptographic algorithms, ranging from authentication to data-at-rest to provenance-preserving logging,<sup>7</sup> are based upon our work on another one of our products, Cryptol,<sup>8</sup> and a host of advanced tools and technologies developed by ourselves and academic partners. Our systems use cryptographically secure authentication and credentials issuance (via technologies like multi-factor authentication), cryptographic databases, cryptographic hardware (including FIPS-certified libraries and hardware), formal protocol design and verification, formally verified cryptographic libraries, and logging with privacy-preserving cryptographic integrity.

For the parts of STAR-Vote that require a cryptographic mix-net, we will use Verificatum AB's mix-net library. We are also likely to use their JavaScript library if we choose to develop a user interface based upon HTML and JavaScript technologies.

In addition to the Verificatum Mix-Net, the cryptographic algorithms we intend to use are AES-XTS, either El Gamal or PPATS (if Travis County does not permit us to use a revised version of the STAR-Vote protocol), and IETF curves and Suite B algorithms for digital signatures and data encryption. Our investigation into the current STAR-Vote protocol has shown that there is a potential security/performance tradeoff between El Gamal and PPATS. Since they serve the same function in the STAR-Vote protocol, we will decide which is the better implementation choice once we can evaluate their behavior in the STAR-Vote system under development.

#### 4.6.5 Other Algorithms

There are a number of algorithms, particularly to fulfill integrity and privacy properties of the STAR-Vote system and to achieve the progress and safety goals of STAR-Vote when viewed as a distributed algorithm, that need to be refined and verified in the course of the STAR-Vote project. We generally summarize these algorithms here.

- **Data-at-Rest:** Some data elements in the STAR-Vote system are not public and have (possibly) varying levels of privacy associated with them. In particular, some data elements are only meant to be visible to election officials (e.g., the election shared public key), other elements are public data (e.g., the contents of a blank ballot), and still other

---

<sup>7</sup> Such as supported in our formally verified election logging framework.

[https://github.com/GaloisInc/Elections\\_Logging](https://github.com/GaloisInc/Elections_Logging)

<sup>8</sup> <http://www.cryptol.net/>

elements are meant to be eternally secret (e.g., voters' intent). As such, cryptographic data-at-rest algorithms are key to fulfilling those security requirements.

- **Distributed Consensus:** The STAR-Vote protocol is, at its core, a distributed algorithm that happens to have cryptographic elements. As such, it needs a bespoke precise specification, as we need to reason about its correctness well prior to implementing it in practice. In particular, the algorithm will have novel safety and progress properties given the nature of a polling place, the network hardware mandated by the RFP, and the assurance properties mandated by the RFP.

#### 4.6.6 *Design and Storytelling Tools*

Our designers and storyteller use a wide set of software to create artifacts used throughout the design and storytelling work. Examples include Adobe's Creative Suite (primarily Illustrator, Photoshop, Premiere, and InDesign), Google's SketchUp, Final Cut Pro for film editing, Autodesk Fusion 360 CAD software, Keyshot rendering software, and Procreate illustration software.

#### 4.6.7 *Design-for-Manufacturing*

**Prototyping Tools.** The kinds of technologies used during prototyping include 3D printing, making models out of wood, paper, textiles, clay, or foam, CNC machining, and laser cutting.

**Design for Manufacturing.** Design for Manufacturing (DFM) describes the process of designing or engineering a product in order to facilitate the manufacturing process and to reduce its manufacturing costs. DFM will allow potential problems to be fixed in the design phase which is the least expensive place to address them. DFM aims to minimize material used, reduce overhead and labor cost, shorten product development time, and focus on standards to reduce cost. Some of the goals in the DFM process are the use of standard parts and materials, use of modular assemblies, minimization of part count, simplification of the assembly process by minimizing the number of manufacturing operations, and specification of surface finishes based on their exact functionality. The technologies used during late-stage design for manufacturing are mainly the same ones used for prototyping.

#### 4.6.8 *Software Backend for Web Services*

N/A

#### 4.6.9 *Hosting Requirements*

N/A

- 4.7 5.7 Describe Proposer's approach to system and software design. Include any development tools and methodologies employed to ensure this project is engineered using best practices and that the resulting system is secure, robust, and scalable. Reference items from Appendix D where possible.

We detail below our rigorous systems engineering and software engineering process and methodology. As with programming languages (discussed above), we make objective decisions about the appropriate tools and technologies for each project or product. Our toolbox, especially in matters related to rigorous systems engineering and applied formal methods, is broader and deeper than that of any other company in the world.



#### 4.7.1 Tools

While we can modify our choices based on input from Travis County, our current plan is to use the following tools: Atlassian or GitHub for distributed version control, change tracking, and development documentation; the Alloy Analyzer and PVS for specifying formal domain models and automatically synthesizing system tests; Boogie and SAW for formal verification of intermediate representations and reasoning; lightweight static checkers of various kinds (e.g., CheckStyle, PMD, and FindBugs for the JVM platform) for ensuring that designs and code are appropriately formatted, well-designed, maintainable, etc.; OpenJML, EiffelStudio, Eclipse with various plugins, Visual Studio with various add-ons, the SPARK Pro tool suite, and the Code Contracts tool suite for performing runtime verification, extended static checking, and full functional verification of implementations against specifications; Coq for formally specifying and reasoning about various formal models of the STAR-Vote system and elections in general; Cryptol for specifying and reasoning about cryptographic algorithms; F\* and Tamarin for specifying and reasoning about cryptographic protocols; Clang and CompCert for compiling C code; various automated theorem provers such as Z3, Lean, CVC4, Yices, and ABC for automatically reasoning about formal models; Emacs, Eclipse, IntelliJ, and other JetBrains technologies, Visual Studio, and SPARK Pro as interactive development and verification environments; CZT, Event-B, Overture, and RAISE for specifying formal models; various compilers to support our languages of choice (e.g., the Dafny compiler, the EiffelStudio compiler, the Rust compiler, the GHC Haskell compiler, etc.); PEX, EiffelStudio, and JMLUnitNG for automatic test code generation; standard test coverage tools such as Jcov and Cobertura; Java Pathfinder and similar model checkers for reasoning about safety properties of implementations; OmniGraffle for drawing system diagrams; the BON and GSSL tool suites for system specification; the Beetlz checker for refinement checking of BON specifications against JML/Java implementations; Mono and .NET Core for a cross-platform .NET runtime; ProVerif, UPPAAL, and the TLA+ tools for distributed algorithm specification and reasoning; and Travis for continuous integration.

#### 4.7.2 Methodology

The specific development methodology we use for all of our software is a variant of Design by Contract<sup>9</sup> with some aspects of a Correctness by Construction<sup>10</sup> approach. Our process, method, tools and technologies span several deployment and development platforms, specification and programming languages, and communication and coordination schemes. In short, we use a combination of the following methodologies, which we explain below in more detail:

- Correct-By-Construction
- Design-By-Contract
- Refinement-Based Process
- Kiniry-Zimmerman Methodology
- Business Object Methodology
- Formal Hardware/Software Co-Design
- Formal Methods (Alloy, CASL, Event B, RAISE, VDM, Z)

---

<sup>9</sup> [https://en.wikipedia.org/wiki/Design\\_by\\_contract](https://en.wikipedia.org/wiki/Design_by_contract)

<sup>10</sup> <https://buildsecurityin.us-cert.gov/articles/knowledge/sdlc-process/correctness-by-construction>

The STAR-Vote design specified in the RFP includes security, fault tolerance for robustness, and scalability. Our software development process emphasizes those same qualities. This type of development process has been used to develop hundreds of millions of dollars' worth of military, aviation, biomedical and financial systems that **must not fail**, because human lives and billions of dollars hang in the balance. We believe that election systems are just as important, because protecting democracy protects human lives and our whole economic system. Our systems are all fault tolerant and have sufficient redundancy, both in algorithm design and physical architecture, to ensure that they can survive the simultaneous failure of multiple machines or networks. We will apply the same high-assurance techniques to ensure that STAR-Vote is developed not only with generic coding best practices (8.1.1<sup>11</sup>) but also with best practices for systems critical to homeland security and medical applications. The system will be far less prone to failure than even the best standard office software (8.3.1).

One important coding best practice for critical systems is performing a machine-checked functional verification of the core algorithms of the software (8.1.1). We first design a mathematical model that is as easily understood as the English language specification. We then provide an implementation that is mathematically proven to meet the specification. This mathematical proof can be automatically checked on a computer, giving unparalleled assurance that the software is correct. These techniques have historically been used for safety-critical systems, where the failure of a system would result in loss of life (e.g., flight control systems at Airbus) or have enormous cost implications (e.g., failure of a mission to Mars).

By combining these techniques, we create a chain of correctness that starts with the high-level system specification and traces down to the smallest implementation details of the most critical parts of the system. At each step in the chain we focus on providing evidence of correctness, generally in multiple forms, including refinement proofs from informal to formal specifications, unit test suites, and mathematical proofs of correctness and security. In other words, all the effort we put into ensuring that our system is correct generates tangible evidence that gives external parties (e.g. certification labs, security experts, political parties, and the American public) the same confidence in our software that we have.

We strictly adhere to well-documented code standards for the various programming languages in which we develop software, and we use appropriate development and testing environments (IDEs, continuous integration systems, issue trackers) to support our development efforts. We aggressively employ techniques such as linting (automated syntactic checks to catch early programming errors), static analysis, and automated testing to provide continuous feedback on our software development practices.

Our formal domain models provide a high-level view of the logical and modular design of the system (8.1.2), ensuring robustness and scalability. From this view, it is easy to see how the components communicate and what their interdependencies are. It is easy to detect components that are too tightly coupled, which would make future replacement or revision challenging; a loosely-coupled system allows for easy extensibility (8.1.4). Our domain models also make it clear what interfaces need to be satisfied by any future module replacement. This means that there is no danger of swapping out a module for a replacement that does not have all the

---

<sup>11</sup> We reference in parentheses the specific section of Appendix D that we address with each part of this discussion.

expected functionality. Once the domain model is satisfactory, we continuously use analysis tools to guarantee that all code we write conforms to the model.

We also create formal models of every data format that we use, both internally and externally. We can use these formal models to generate software that allows a variety of programming languages to communicate natively via our data formats, providing fluent interoperability (8.1.4).

Our proposed design is highly modular (8.1.2). Each module uses only open data formats for communication, resulting in a system that can easily integrate with third party systems and can be modified and upgraded by anyone who is familiar with the data formats. A modular architecture assists with validation and verification, allows for experimentation with user experience variants, and enables phased user acceptance testing. It can also ease customization of the system, allowing new voting methods and ballot styles to be swapped into the system as needed without requiring system-wide changes. Modular design also aligns with what we expect to see in version 2.0 of the U.S. Election Assistance Commission's Voluntary Voting System Guidelines.

Our development repositories contain the code under development, the full set of development artifacts described above, and unit, performance, and integrated functional test suites for each subsystem and for the system as a whole. Our test servers pull from these repositories and perform automated builds and testing whenever code is updated. In addition to standard functional tests we place a particular emphasis on performance tests, which allow us to ensure that feature changes do not impact performance (8.6).

The artifacts we produce during system development provide assurance about the functionality and security of our systems that cannot be matched by any existing elections system. They also serve as comprehensive documentation (8.1.3) and test suites that can be submitted as part of the federal and state certification process. As a result, certification can be dramatically cheaper and faster for our systems than for systems created by other vendors. For example, an election tabulation system built by a team led by Dr. Kiniry and used in The Netherlands for the 2004 European Council Elections was developed and certified within 12 calendar weeks, instead of the year or more typical for election systems in that country at that time.

This applies to system revisions and customizations as well: the unchanged parts of the modified system retain their original assurance evidence, and the new assurance evidence related to the modifications allows the modified system to be recertified quickly and inexpensively.

Historically, this kind of system has been evaluated in an ad hoc manner based upon informal requirements documents, a repository of source code, a User's Manual, and some examples of its use. By contrast, our rigorous system design and assurance tests are derived systematically from the client requirements. For elections, these requirements include County specifications and the governing election law.

Our rigorous systems development method for the aforementioned Dutch election system produced three particularly useful artifacts: (1) a formal specification of the domain model of Dutch elections, (2) a formal architecture description, and (3) a model-based design-by-contract specification of the system.

Producing item (1) revealed over one hundred errors in Dutch election law and the election system that we were asked to integrate with. Catching these errors engendered confidence that the system we created fulfilled the requirements stipulated in law.

Item (2) let the team decompose the development work into three strictly separated subsystems (UI, I/O, and core data types and algorithms), implement and verify those subsystems completely apart from each other (this is called compositional verification), and plug them together at the end of the project, resulting in a system that operated correctly the very first time it was executed. This decoupling permitted the team to parallelize work, avoiding inefficiencies related to inappropriate relationships between subsystems, and let us ensure that the implementation of the system conformed to its architecture, avoiding what is known as architecture drift.

Item (3) helped achieve greater assurance faster than any traditional engineering approach. In particular, our methodology enabled the team to automatically generate unit, subsystem, and integration tests from model-based specifications, saving an enormous amount of time over hand-written tests. Additionally, we provided assurance about the consistency and coverage of those tests against election law and client requirements because we were able to trace tests all the way from law to code. Finally, we used those specifications to formally verify that the implementation behaved correctly under all possible inputs. We performed this verification using an advanced static analysis technique known as extended static checking, a technology for which Dr. Kiniry and other team members are internationally recognized.

The assurance artifacts provided in that project for the Dutch government over a decade ago are significantly more advanced than what any election systems vendor (other than Free & Fair) provides today. Our rigorous process enabled an extremely efficient certification process then, and will do the same for STAR-Vote.

#### 4.8 5.8 Describe the process and any tools used for configuration management for control of source code, methods for continuous integration for automated build and testing and any tools used for defect tracking and reporting. Also address methods used for version control and tracking of documentation.

Development follows a continuous integration, continuous deployment approach. Each code change is tested automatically, as soon as it can be, to catch defects as early as possible. Continuous integration is a proven way to reduce development cost and improve productivity. In continuous deployment, code that has passed integration testing is promoted automatically from the main development branch to a deployment staging area that allows all project personnel to access and test the latest working code in a whole-system context.

We have experience working with both external build tools, such as Travis CI, and internal build tools like Jenkins. We will work with Travis County to determine what solution is best for this project, but no choice will significantly change the functionality of our continuous integration approach. As mentioned elsewhere, we will break development into approximately weekly tasks. These tasks will be completed by commits to the main branch of the development repository. With this setup, if we wish to report progress to Travis County, we must integrate the changes first. This allows both Free & Fair and Travis County to take maximal advantage of the continuous integration approach.

Documentation and commenting is interwoven with development (8.1.3). Beginning with our formal domain models, we lay out the requirements and expectations of each module. We do this

both formally (in a language that we can automatically check later) and in plain English. Moving forward, we translate both of these specifications into appropriate constructs (documentation comments, assertions, annotations, type specifications) in our programming language of choice. This enables the automatic generation of PDF and HTML documentation describing each piece of the software and showing relevant code snippets.

We typically use Git for version control (8.1.5), within GitHub or a similar environment that provides commit hooks (for automatically running testing tools, static checking tools, etc. every time the codebase is changed) and issue tracking. We are open to using any other industry standard version control solution desired by our clients, as long as it supports continuous integration and issue tracking. Also, some of the design tools we enumerated earlier have built-in sharing and version control capabilities. We intend to leverage those capabilities and have snapshots of design artifacts captured in our distributed version control system like any other engineering artifact.

When a defect is noticed either by Free & Fair or Travis County, it will be immediately logged in the issue tracking system. Within a day of entry to the system, each issue will be categorized and assigned to a team member who will be responsible for driving the effort to fix the issue. Each code change that has an effect on an issue will reference that issue, so that progress towards a fix can be observed as it occurs. We will maintain a policy that an issue can only be closed once the party that raises the issue signs off that the issue has, in fact, been fixed.

All development-related team communication is facilitated by a wiki that is accessible to and editable by all team members. This wiki also serves as the reporting facility for team metrics and the home of software documentation during development activities. We use metrics such as test suite success rate and defect escape rate to monitor code health, adapting our test suites and design review processes to meet goal lines for each metric.

If Travis County wishes to contract us for ongoing upgrades to the system, we will use Ansible or a similar configuration management tool to ensure that environments remain consistent across machines. Note that, since configuration management exists for the convenience of the client, we are comfortable with any variety of configuration management tools (such as CFEngine, Puppet, Chef, etc., as appropriate for the given programming language and deployment platform) and will work with Travis County's IT department to come to a suitable solution.

Finally, we can also package and deliver full snapshots of development environments in virtual machine images. We typically use VirtualBox for such work.

#### 4.9 5.9 Describe the process for transitioning from a test environment to a production environment.

Free & Fair develops open source software systems in full public view. Therefore, all artifacts associated with a given project or product are immediately available to all stakeholders, at any time, via a web-based collaborative development environment such as GitHub. This means that various versions of the same system (e.g., builds for various platforms, experimental branches in which new features are being explored, etc.) are immediately available to anyone who browses the project website and clicks on the right download link, or clones the repository and builds it for themselves.



Delivery of production systems to a client or stakeholder is accomplished by providing the modern equivalent of “golden master disks” of yesteryear. The nature of these deliveries differs according to decisions made during contracting and development, in tandem with the client.

For example, if the deployment platform is a flavor of Linux, one of the standard software packaging systems such as RPM or dpkg is used to deliver products. If the deployment system is Microsoft Windows or macOS, the standard open source packaging software is used to deploy production systems.

We believe that the deployment of a certified version of a product to hundreds or thousands of devices requires a different mechanism than the traditional “hire dozens of interns to do everything by hand.” While the details of such a deployment depend significantly on industrial design decisions, we are inclined to use a public large-scale parallel export of (cryptographically forensically checked and signed) product masters onto COTS SD cards for manual insertion in all systems. Such a deployment mechanism would use inexpensive media that is long-lasting, easy and cheap to archive, and would be designed to address our deep concerns with regards to the deployment and auditing of certified product versions. Travis County could then archive all of the digital materials relevant to an entire election in one small lockbox or safe deposit box.

Finally, there is a transition scheme from the test environment to a production environment for hardware. That phase transition moves from ideas witnessed in a small number of prototypes to a solution that can be manufactured at high quality with low cost. The main challenges inherent in that transition are scalability (from the testing lab to the product launched on the market) and the means by which open hardware design can work effectively in the open source marketplace (a relatively new idea).

#### 4.10 5.10 Propose a structure for providing ongoing support, maintenance, and upgrades to the system.

We propose an annual contract with a Service Level Agreement (SLA) for technical support for Travis County staff using the system.

No maintenance contract is required. In the event of a software defect—unlikely because of our high assurance development techniques—Free & Fair will fix the defect at no charge to Travis County. In the event of hardware defects, any COTS parts can be easily replaced. Or Travis County may wish to obtain a service plan from their COTS hardware vendor(s).

No upgrade contract is required. Free & Fair will not require Travis County to upgrade the software to maintain the functionality provided as part of this procurement. Any necessary work to package and install future versions, should Travis County elect to upgrade, can be included in the annual SLA contract with Free & Fair. During contacting we can detail exactly what such an SLA covers.

In the event that Travis County requires specific software upgrades (e.g., to comply with changes in election law), the County can reasonably choose to solicit bids for each particular upgrade project. Open source software allows a variety of vendors to compete for upgrade work, so no single vendor can depend on proprietary lock-in.

Because Free & Fair proposes software designed to work on any operating system, operating system upgrades or security patches should not adversely impact the software. In the unlikely



event that the software is adversely affected by an operating system patch or upgrade, the County can reasonably choose to solicit bids for each particular upgrade project.

- 4.11 5.11 Equipment in the polling location must remain operational on battery power for at least four hours. A full precinct must be able to be operated by the power provided by a typical gas-power generator supplying about 2000 watts. Propose a test protocol to demonstrate this system capability.

Our proposed system will not need any external power to stay powered on for 4 hours. The UPS units and printer batteries will last for at least 4 hours using the hardware we have recommended, even at full utilization. To ensure this, we will include a power test program that uses significant processor, monitor, and printer resources. If this program can run for the required amount of time on battery power, it will guarantee that the system will run for that amount of time on battery power under any live polling place conditions.

- 4.12 5.12 Propose a file specification and transfer method for a configuration import file produced by the In-Person Voting/Tabulation Election Definition Import and Finalization module to initialize the Ballot Box/Scanner prior to the election to meet the functional and operational requirements and descriptions for the Ballot Box/Scanner as defined in this RFP.

The configuration file used to initialize the Ballot Box/Scanner will have the same format as the configuration file provided to the In Person Voting/Tabulation Election Definition Import and Finalization module, even though the Ballot Box/Scanner will not make use of most of the configuration information in that file.

In general, we have no preferred data file specification, beyond our own open formats which we are proposing for evaluation to relevant VVSG 2.0 working groups, for exporting data to third-party systems. In general, our preference is for data file formats that are both human and machine interpretable, have a precisely defined syntax and semantics, and are unencumbered by any IP or patent concerns.

We can use any standard interface for exporting data to a third-party system as long as the third-party data format is open and has an associated specification language. Two examples of such open formats are JSON (with JSON schemas) and serialized Google Protocol Buffers. Assuming that Element C is running on hardware substantially similar to our hardware recommendations, our preferred interface would be to export data to files on an SD card. If the third-party system cannot specify such a format directly, we can create either a standalone application or a file translator module, integrated with the election definition export system, to translate the open format file specification into the third-party's input specification. In general, we advocate for interfaces that support cryptographic data integrity and provenance, will continue to be in use into the indefinite future, and do not depend upon a small number of suppliers (i.e., we have learned a lesson from other vendors' use of ZIP disks, floppy disks, etc.).

- 4.13 5.13 Propose a bi-directional data interface between the Ballot Control Station (BCS) and the Ballot Box/Scanner (Element C).

The interface will be the local area network to which both devices are connected.

All messages between the BCS and the Ballot Box/Scanner will follow a well-defined format, specified with Google Protocol Buffers.

4.14 5.14 Propose a data file specification and interface for transferring the Ballot Box/Scanner election data following the close of polls to the Back Up and Archiving module defined in Element B of this RFP.

We can use any data file specification, as long as that specification is open and has an associated specification language.

With regard to preferred data file specifications and interfaces, our answer for this section is the same as for Section 4.12.

4.15 5.15 Proposals must include a list of all consumable supplies necessary for the proper operation of the voting system, including estimated usage rates and costs.

There are two primary consumables associated with the voting system. First, there are data storage devices used to configure voting systems and store digital election results. Second, paper is used for voting tickets, ballots, status reports, and similar output.

**Data Storage.** The details of what digital data storage mechanism is used in both the Element B (in-person voting and tabulation) and Element C (ballot box/scanner) systems will, in the end, be largely based on industrial design decisions. However, we are inclined to use a public large-scale parallel export of (cryptographically forensically checked and signed) product masters onto COTS SD cards for manual insertion in all systems. Such a deployment mechanism would use inexpensive media that is long-lasting, easy and cheap to archive, and would be designed to address our deep concerns with regards to the deployment and auditing of certified product versions. Travis County could then archive all of the digital materials relevant to an entire election in one small lockbox or safe deposit box.

As such, when purchased in bulk, SD cards that can hold the entirety of the necessary operating system stack and STAR-Vote system are on the order of \$10 each. Consequently, using the volume estimates provided in the RFP for deployment systems for the county, 2,000 voting systems and 500 ballot box/scanners necessitate at least 2,500 cards. Adding in sufficient excess for potential media failures, we arrive at an estimated cost of \$26,000 per election for data storage.

**Paper.** If Travis County elects to use direct thermal printing, which was indicated as a preferred technology in the RFP, the only consumable supply necessary for proper operation of the voting system is thermal printer paper for printing ballots and voting tickets.

When purchased in bulk, thermal receipt paper for printing voting tickets with a standard receipt printer, such as the one we recommended in the response to requirement 0, costs approximately 0.35 cents (\$0.0035) per linear foot in rolls of 200 feet. Assuming that each voting ticket is at most 3 inches high, that yields a cost of approximately 0.11 cents (\$0.0011) per voting ticket, or approximately \$1.10 for 1000 voting tickets. In the most recent general election in Travis County, nearly 500,000 voters cast ballots; given similar turnout, and assuming every voter casts a vote at a polling place, voting ticket paper for a single general election would cost approximately \$550.00.

Thermal paper for ballots is more expensive because of the limited number of suppliers of letter and legal size thermal paper. A standard 21lb weight sheet of archival quality letter size thermal paper costs approximately 10 cents. Thus, printing 500,000 ballots would cost \$50,000. The use

of specialty paper with security features, or a thicker paper weight, could significantly increase this cost depending on the specific features and paper weight desired by Travis County.

Note that any excess paper that is not used in a particular election can be used in the next election, and is not wasted as consumables for other printing technologies (e.g., inkjet printer cartridges) might be.

## 5 Part II, 6.0 Detailed Response: Element C

We propose to develop **Element C, Option 1** of the RFP.

We will develop an interim functional Ballot Box/Scanner system that is an assembly of COTS hardware. While it will be functional, it will not be as robust, usable, and accessible as our custom STAR-Vote Ballot Box/Scanner, discussed below. Our component price for the interim solution includes all of its software and the hardware to build exactly one demonstration unit.

We will also develop a custom STAR-Vote Ballot Box/Scanner, custom hardware for ballot paper feed and scanning, and associated software. This work will be conducted in tandem with a hardware design firm (Design SHIFT) whose expertise is directly relevant to user-centric, secure public devices. Our usability and accessibility experts will ensure that the physical design of the Ballot Box/Scanner is usable by all voters and election officials and accessible to disabled voters. In support of this effort, our team will develop a Virtual Reality (VR) environment of the system early in the design phase to obtain continuous feedback from our team and customer stakeholders and ensure an optimal design.

### 5.1 6.0 Propose a file specification and transfer method for a configuration import file produced by the In-Person Voting/Tabulation Election Definition Import and Finalization module to initialize the Ballot Box/Scanner prior to the election to meet the functional and operational requirements and descriptions for the Ballot Box/Scanner as defined in this RFP.

The configuration file used to initialize the Ballot Box/Scanner will have the same format as the configuration file provided to the In Person Voting/Tabulation Election Definition Import and Finalization module, even though the Ballot Box/Scanner will not make use of most of the configuration information in that file.

We can use any standard interface for importing data from a third-party system as long as the third-party data format is open and has an associated specification language. Two examples of such open formats are JSON (with JSON schemas) and serialized Google Protocol Buffers. Assuming that Element B is running on hardware substantially similar to our hardware recommendations, our preferred interface would be to import data from files on an SD card. If the third-party system cannot specify such a format directly, we can create either a standalone application or a file translator module, integrated with the configuration import system, to translate the third-party's output specification into the open format file specification. In general, we advocate for interfaces that support cryptographic data integrity and provenance, will continue to be in use into the indefinite future, and do not depend upon a small number of suppliers (i.e., we have learned a lesson from other vendors' use of ZIP disks, floppy disks, etc.).

### 5.2 6.1 Propose a bi-directional data interface between the Ballot Control Station (BCS) (from Element B) and the Ballot Box/Scanner.

The interface will be the local area network to which both devices are connected.

All messages between the BCS and the Ballot Box/Scanner will follow a well-defined format, specified with Google Protocol Buffers.

**5.3 6.2 The successful proposer for Element C is required to work with the Red Team from Element D. Provide an outline of a plan for working with the Red Team.**

The Element D Red Team will have full access to our source code and hardware designs, and will not be limited to “black box” interactions with the system. They will have full access to our development repositories, and will be able to submit reports to us directly via a bug tracking service. This will allow interested parties to follow any discoveries made by the Red Team and see what action has been taken on any individual issue, as well as to check whether any issues have been resolved.

In addition, we have planned multiple design iterations, which will be available to the Red Team for in-depth testing and analysis.

If any issue reported by the Red Team does not come associated with code to exercise the issue, we will create that code; thus, when each issue is fixed, we will be able to point to a specific revision of the software that contains visible evidence that the issue has been fixed. Continuing to maintain such examples will also ensure that further modifications to the software don't reintroduce any issues discovered by the Red Team.

If desired, the Red Team can also interact with us directly during and after system development via multiple collaboration mechanisms (telephone, email, instant messaging, and videoconferencing).

**5.4 6.3 Describe the various technologies proposed to be used during any development, including: programming language(s)/software libraries; test frameworks; algorithms (where these aspects are unusual or important to the design, including the selected cryptographic algorithms); and software backend for web-services and any implied hosting requirements.**

Please see Section 4.6.

**5.5 6.4 Describe Proposer's approach to system and software design. Include any development tools and methodologies employed to ensure this project is engineered using best practices and that the resulting system is secure, robust, and scalable. Reference items in Appendix D where appropriate.**

Please see Section 4.7.

**5.6 6.5 Describe the process and any tools used for configuration management for control of source code, methods for continuous integration for automated build and testing and any tools used for defect tracking and reporting. Also address methods use for version control and tracking of documentation.**

Please see Section 4.8.

**5.7 6.6 Propose a data file specification and interface for transferring the Ballot Box/Scanner election data following the close of polls to the Back Up and Archiving module defined in Element B of this RFP.**

We can use any data file specification, as long as that specification is open and has an associated specification language.

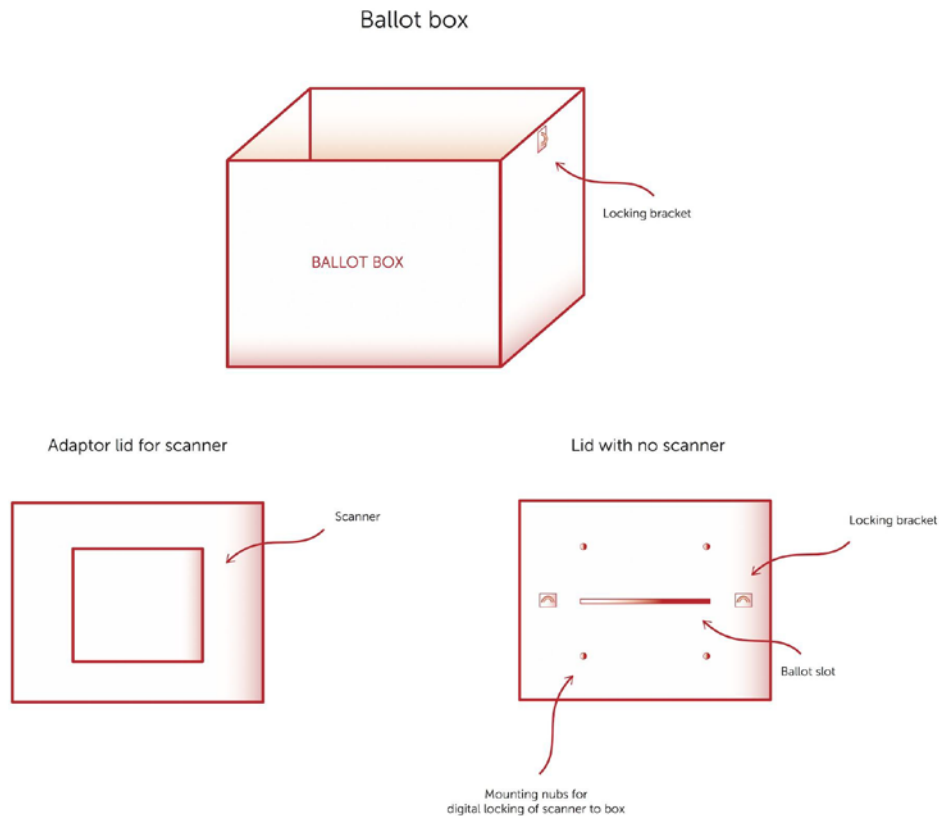
We can use any standard interface for exporting data from a third-party system as long as the third-party system accepts data in an open format with an associated specification language. Two examples of such open formats are JSON (with JSON schemas) and serialized Google Protocol Buffers. Assuming that Element B is running on hardware substantially similar to our hardware recommendations, our preferred interface would be to export data to files on an SD card. If the third-party system cannot accept such formats directly, we can create either a standalone application or a file translator module to parse the third-party output and translate it to an open format.

5.8 6.7 Ground-up development: If proposing the development of a new Ballot Box/Scanner hardware device (Option 1 from RFP Appendix F, Hardware Requirements, Section 10.9), provide the following:

5.8.1 6.7.1 *Rendering of the proposed mechanical design and a description of the mechanical functions;*

We have rendered a handful of design sketches that include mechanical design components. The primary mechanical functions highlighted in our design sketches are annotated on the figures.

Our Ballot Box itself (Figure 6) is just a simple, secure ballot box like those the County currently uses. It needs some form of physical locking bracket so that a keyed lock can be used by elections officials to secure the adaptor lid to the box. Note that the box with attached lid but no scanner is just a normal secure ballot box, and can be used for traditional (non-STAR-Vote) elections.



*Figure 6: Ballot Box*

Scanner devices, as seen in Figure 7, lock to the Adaptor Lid using digital locks and mounting nubs. These locks are active when there is no power, thus removing power or discharging the battery does not expose ballots to tampering. The housing hides all COTS compute, scanning, power, and communication components as well as the mechanical subsystem that friction feeds ballots into the scanner. An LCD is used to provide feedback to the voters about the state of their ballots and ballot submission sessions. Ballots are fed into the front of the Scanner via the feed tray, and accepted ballots feed out of the scanner and into the Ballot Box via the slot in the Adaptor Lid. Access to the SD card to configure the system and export data is located under a digitally locked access panel on the bottom of the Scanner.



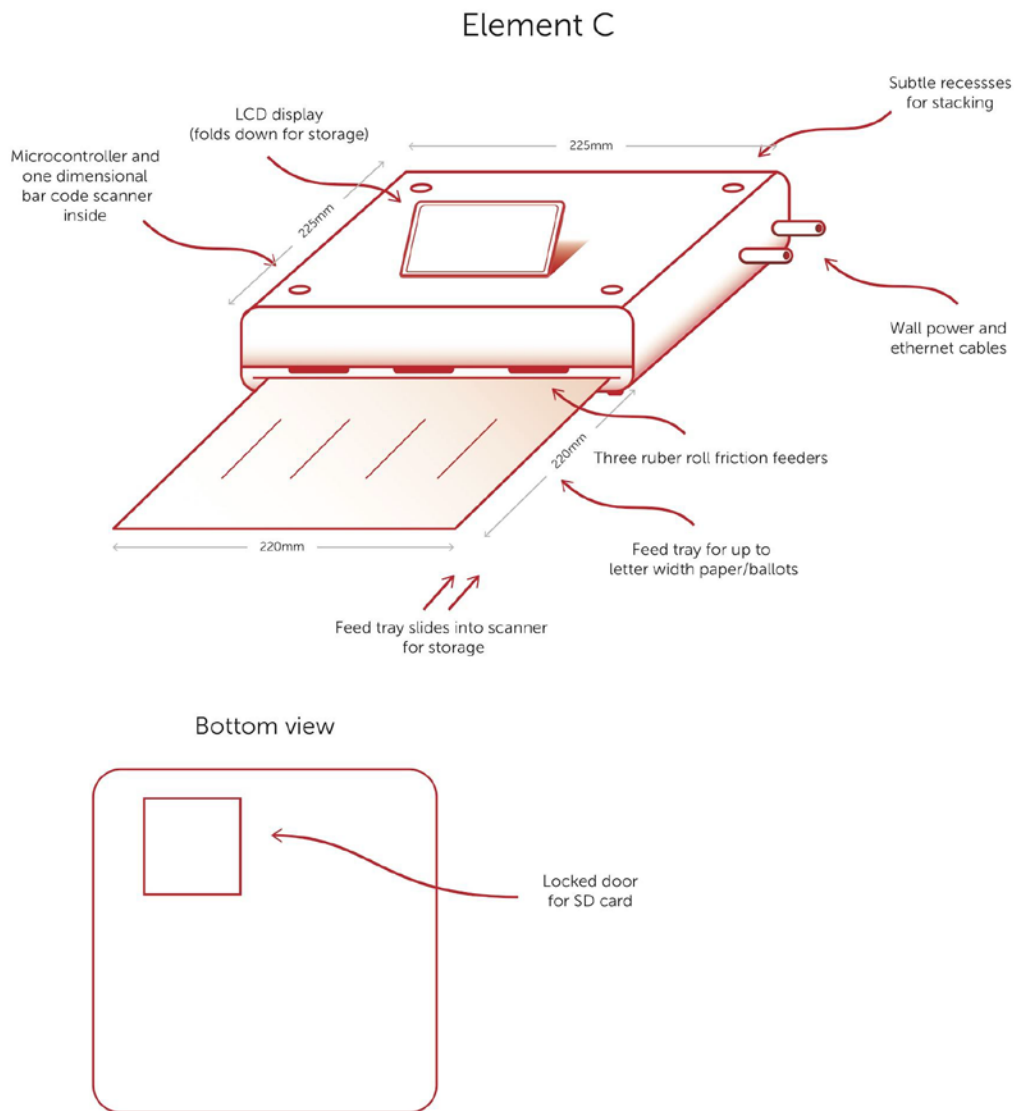


Figure 7: Scanner Device

**5.8.2 6.7.2 Describe the electrical and mechanical design, engineering, development and testing process. Testing should include mechanical stress testing and highly accelerated life testing.**

Our design process consists of the following phases, with respective tasks and reviews:

- Scoping
- Detailed design
- Testing
- Production ramp
- Certification
- Release to market

**Scoping.** In the scoping phase, a number of industrial design (ID) concepts are created in alignment with the product requirements. Some requirements explicitly originate from the client, some are derived requirements coming from additional in-depth studies on system use cases as well as usability studies. The product's electronic architecture is defined based on functional requirements and non-functional requirements such as security and performance goals. The preliminary target Bill of Materials (BOM) is derived from this architecture. The necessary engineering and project management resources are then captured in a resource plan and combined with a schedule and first budget estimate.

**Detailed design.** During the detailed design phase, the final ID is used to start the Mechanical Engineering (ME) of the product. As shapes and Color Materials Finishes (CMF) are locked down, structures and features are put in place to make manufacturing of the parts possible and to securely fix all components. Design variants explored in this phase are rendered into the VR environment for feedback from stakeholders. During this product integration, all parts are fixed in the main shell of the product. The selection of electronic components (Electrical Engineering, or EE) is finalized and the first hardware prototypes are built. If any custom software is required, a prototype version is created to demonstrate the basic required functionality. Once principal functionality is established, the EE and ME BOM is finalized.

**Testing.** The overarching goal of this phase is to test as much as is useful as early as possible. Recall that ID and UI prototypes are tested using models as simple as drawings and paper prototypes; but in this phase, we focus on the physical product throughout development.

We begin with basic fit and interference of mechanical parts in mock-ups which are created via 3D printing, SLA, or machining of plastics and metals. These mock-ups also accommodate some basic functional and usability experiments and feedback.

We then introduce electrical verification, which includes signaling and some electromagnetic compatibility pre-testing. It also can be the start of testing for thermal dissipation at an assembled system level, confirming component temperatures stay within specifications for reliability and that surface temperatures are appropriate for comfort and safety.

Next, we typically introduce mechanical parts made with hard tools. These are considered representative of final parts and trigger much more in-depth physical testing including operational and storage temperature range testing, vibration testing, drop test, water and dust ingress testing, and testing of part fit (gaps, steps, bulges), finishes including production marks, textures, paint quality (appearance and reliability), surface hardness, and printing appearance and reliability. As failures are identified, solutions are prototyped and verified.

As the product is polished, the difficulty of testing escalates to include combinations like Highly Accelerated Life Test (HALT), where we combine factors like temperature extremes and vibration in order to try to force early failures and identify long-term system weaknesses. At the same time, with fully tooled physical parts using final materials, we can have confidence that the electromagnetic compatibility testing is reflective of what we will see in production, so these units are submitted to labs for formal certification testing (see below). Finally, late in this phase we would typically introduce packaging, which brings with it transportation testing of the packaged product.

**Production Ramp.** This phase is intended to finalize the product in all aspects of engineering while making sure all required cases are testable. The detailed definition of test processes happens in this phase as well.

Engineering Validation Test and Development Validation Test both happen in this phase. Each requires a different level of functional correctness as well as dimensional accuracy, visual appeal and surface quality. Detailed Test plans are established here, assuring a smooth ramp into a production environment. Reliability tests and product Q/A is done at this time, and minor adjustments are fed back to the design based on the respective findings. If compliance tests are required for the product, they are also implemented in this phase. These are usually executed by third parties. If any custom software is required for this product, test releases of production code are also delivered at this time. Any required certification will be kicked off in this phase.

**Certification.** Certification concerns are addressed throughout the project, beginning to end. Requirements and guidelines from Voluntary Voting System Guidelines and accessibility considerations will drive features from day zero. Wherever possible, other certifications will be checked at as early a prototype level as is meaningful, such as early testing of electromagnetic compatibility. Final formal certification will be completed at the end via accredited and approved third-party labs. UL listing, though not a legal requirement, will be obtained as proof of engineering best practices with respect to product safety.

**Release to market.** No functional changes to the hardware are allowed in this phase, and no substantial ME changes are allowed in this phase, as this is intended to develop and tune the manufacturing and test process to their maximum efficiency. The detailed design engineering is brought to an end in this phase and test processes and fixtures are developed to allow for efficient and complete testing of the product.

The product is validated to be to specification in order to be released to production. Any support required by the manufacturer to be able to ramp to full scale production will be provided in this phase. The complete design ownership is usually transferred to the manufacturer in this phase after a review with the customer and sign off.

#### *5.8.3 6.7.3 Describe an interim solution for processing PVRs including the mechanical configuration and software interface.*

For an interim solution, we recommend a COTS hardware solution that uses an Arduino-compatible microcontroller coupled to a COTS laser barcode scanner, an LED display to give the voter feedback, and a driver motor in a COTS paper feeder whose output feeds directly to the client's ballot box. We have already built an in-house prototype of such an interim product that uses LEGO bricks and a LEGO Mindstorms kit as the assembly, physical housing, and microcontroller. We do not recommend deploying such a system—this was only built to experiment with subsystems in the absence of a more robust housing. We can fabricate interim hardware housing in any number of ways, including in a woodshop, metalwork, 3D printing, etc. We can produce a small number of interim hardware devices for prototyping and demonstration purposes.

**5.8.4 6.7.4 Outline of the manufacturing process and cost of goods once in production. An initial production run of 500 units should be used to calculate cost projections.**

**Mechanical parts process.** Molds are needed for the process of injection molding most of the custom plastic parts for the ground-up Ballot Box/Scanner (not the interim solution). The cost of designing and producing the molds is a one-time cost for the production.

As the number of parts is relatively small, we will be able to use soft molds, which are cheaper to build. These molds are good to produce a maximum of 5,000 parts. If higher quantities are required, either another soft mold will need to be produced or a hard mold can be chosen at a significantly higher upfront cost for production. The cost of the respective mold is due before the first part can be produced this way.

The cost of this mold can be split into two parts: (1) designing the mold, and (2) manufacturing the mold. As a consequence, repeat orders of the same mold will be slightly cheaper than the initial mold. To start production of the parts, the vendor usually requires payment of the full amount due before production can start.

We have obtained preliminary quotes from several manufacturers for the components necessary to create portable, private in-person voting booths, a basic secure enclosure for the In-Person Voting/Tabulation system, and the Ballot Box/Scanner. All initial quotes are in alignment with our goal of having systems manufactured, assembled, and shipped to Travis County at a cost of approximately \$1,200 for each In-Person Voting/Tabulation system and \$500 for each Ballot Box/Scanner.

**Electrical parts process.** As the main electrical parts are COTS, a regular purchase process is applicable here. All funds will need to be made available at the time of purchase, then the fulfillment process can start.

**5.9 6.8 Describe the process from transitioning from a test environment to a production environment.**

Please see Section 4.9.

**5.10 6.9 Propose a structure for providing on-going support, maintenance, and upgrades to the system.**

We propose an annual contract with a Service Level Agreement (SLA) for technical support for Travis County staff using the system.

The only maintenance contract needed would be for non-COTS custom hardware components in Element C. Note that because the hardware specifications are open source, this maintenance contract can be bid competitively.

In the event of hardware defects, any COTS parts can be easily replaced. Or Travis County may wish to obtain a service plan from its COTS hardware vendor(s).

In the event of a software defect—unlikely because of our high assurance development techniques—Free & Fair will fix the defect at no charge to Travis County. In the event of hardware defects, any COTS parts can be easily replaced. Or Travis County may wish to obtain a service plan from their COTS hardware vendor(s).

No upgrade contract is required. Free & Fair will not require Travis County to upgrade the software to maintain the functionality provided as part of this procurement. Any necessary work to package and install future versions, should Travis County elect to upgrade, can be included in the annual SLA contract with Free & Fair. During contacting we can detail exactly what such an SLA covers.

In the event that Travis County requires specific software upgrades (e.g., to comply with changes in election law), the County can reasonably choose to solicit bids for each particular upgrade project. Open source software allows a variety of vendors to compete for upgrade work, so no single vendor can depend on proprietary lock-in.

Because Free & Fair proposes software designed to work on any operating system, operating system upgrades or security patches should not adversely impact the software. In the unlikely event that the software is adversely affected by an operating system patch or upgrade, the County can reasonably choose to solicit bids for each particular upgrade project.

5.11 Provide detailed responses to the applicable items in Appendices D, E, F and G.

See also Section 11, RFP Appendix D; Section 12, RFP Appendix E; Section 13, RFP Appendix F; and Section 14, RFP Appendix G.

## 6 Part II, 9.0 Contractor Requirements

All requirements of Part II, Section 9, are **acknowledged**.

## 7 Part II, 10.0 Contract Requirements

All requirements of Part II, Section 10, are **acknowledged**.

## 8 Part II, 11.0 Maintenance/Service Level Requirements

All requirements of Part II, Section 11, are **acknowledged**.

## 9 RFP Appendix B: In-Person Voting/Tabulation

All requirements of Appendix B not mentioned in this section are **acknowledged**.

*2.5.1.4 The operating system(s) that runs(s) the various software programs must be specified in the proposal and must:*

- *Qualify as COTS;*
- *Not unduly restrict hardware component choices;*
- *Be able to have general system settings managed and locked down by a network administrator;*
- *Not be changed in a way that would invalidate its qualification as COTS;*
- *Run on a common operating system to minimize training costs;*
- *Support Measured Boot or equivalent technologies enabled by a hardware or firmware Trusted Platform Module (TPM).*

**Acknowledged.** Our software is in no way limited to running on an individual operating system. We will deliver and support an instance of our software intended for use on any

reasonable operating system that Travis County desires. Examples of “reasonable” operating systems include but are not limited to Windows 10, Ubuntu Linux, Fedora Linux, FreeBSD, and macOS.

We recommend running all software on Ubuntu Linux, which is open source and free to install. Commercial support solutions are available for Ubuntu at a price that is much lower than the comparable price for Windows or another closed-source operating system. Ubuntu Linux offers a minimal installation as a simple configuration option at setup time, using a COTS installer. *So Ubuntu Linux qualifies as COTS.*

Ubuntu Linux can run on almost any system that Windows can run on, so *Ubuntu Linux does not unduly restrict hardware component choices.*

Ubuntu Linux is common enough that any network administrator will have no difficulty with configuration. *The general system settings for Ubuntu Linux can be managed and locked down by a network administrator.*

Ubuntu Linux *would not need to be changed in any way that would invalidate its qualification as COTS.* Ubuntu Linux is common enough to *minimize training costs.* Ubuntu Linux *supports Secure Boot, a technology equivalent to Measured Boot.*

*2.6.1.7.4.2 Provide an intuitive, graphical, dashboard-style interface with meaningful information for election workers to use. This includes the status of each connected device, grouped by Device Role including a battery indicator (that very clearly indicates if the device is running on battery power, and its level of charge).*

**Acknowledged with interpretation.**

If Travis County implements our recommended hardware and operating system, then this requirement is accepted and included in the cost proposal. Other choices of hardware or operating system may require reevaluation of this requirement.

*2.6.4.4 Detect the presence of one or more connected batteries, and provide information on the BCS's power state to the poll worker (charging/discharging/connected, % power remaining, etc.). The batteries powering the network switches must be connected to a BCS station to be monitored, and must be able to be identified and displayed individually.*

**Acknowledged with objection.**

**Alternate Wording:**

*Detect the presence of one or more connected batteries, and provide information on the BCS's power state to the poll worker (charging/discharging/connected, % power remaining, etc.). It must be possible to individually view status information about each battery powering the network switches.*

**Implementation Approach:**

We would like to further discuss this requirement and devise a feasible solution that meets the needs of Travis County. In the meantime, we propose to use an uninterruptible power supply (UPS) with USB communication for each BCS, and to either attach the



UPSs for the network switches to nearby voting stations or ballot boxes or use UPSs with visual status indicators for the network switches.

**Justification:**

Monitoring every battery in the system, particularly those powering the network switches, presents a significant challenge with regard to wiring and maintaining connections. UPS devices with Ethernet connectivity are quite expensive relative to other UPS devices with the same battery capacity, and USB cable length limits make it impractical to run long USB cables to the BCS from UPS devices powering the network switches.

*2.7.1.2 Accept a Digital Certificate specific to this device used to sign all outgoing network messages.*

**Acknowledged with objection.**

**Alternate Wording:**

*Generate a secret signing key (sometimes called a “Digital Certificate”) or accept an externally-generated secret signing key specific to this device used to sign all outgoing network messages.*

**Implementation Approach:**

Decentralized generation of secret signing keys.

**Justification:**

While each machine will certainly have a secret signing key (sometimes called a “Digital Certificate”), having the machine generate such a key on its own rather than accepting one that is generated externally will meet the same security goal and may ease implementation.

*2.7.2.2.2 If not authenticated, refuse to accept messages from the device, and do not send messages to the device.*

**Acknowledged with objection.**

**Alternate wording:**

*If not authenticated, refuse to accept messages from the device.*

**Implementation Approach:**

N/A

**Justification:**

It is our understanding of the network layer that all messages are broadcast to the entire network. As such, while the network layer will not accept messages from unauthenticated devices, the design does not allow it to prevent sending messages to unauthenticated devices.

*2.7.3.11 Detect any error event or state that could adversely affect the ability of the Voting Station to function properly.*

**Acknowledged with objection.****Alternate Wording:**

*Detect error events or states that could adversely affect the ability of the Voting Station to function properly.*

**Implementation Approach:**

N/A

**Justification:**

While we will do our best to detect such states, in rare cases certain hardware failures and certain other events cannot be detected reliably because they are too unpredictable and have such a wide range of possible effects. For example, a processor failure could cause the system to operate incorrectly and simultaneously render any error detection software inoperable. Such failures are rare, not easily predictable, and generally result in such significant disruption that the entire machine becomes unreliable. As such, we cannot agree to write software that will detect *any* error state. We will be happy to refine this requirement with Travis County at the time of contracting.

We also note that the design of STAR-Vote ensures that no failure of hardware or software will be able to subvert the verification procedures. While this is not cause to abandon error detection, it all but eliminates any fear that a hardware or software failure will cause an undetectable failure to represent voter intent.

*2.7.5.5 Detect and disallow printing to non-physical print devices (such as PDF printers or other virtual printers).*

**Acknowledged with interpretation.**

This requirement is achievable, provided that it is acceptable to limit printing to a specific device (or to a specific device driver) prior to the election.

## 10 RFP Appendix C: Support Modules

All requirements of Appendix C are **acknowledged**.

## 11 RFP Appendix D: Software Specification

All requirements of Appendix D are **acknowledged**.

## 12 RFP Appendix E: Cryptography

All requirements of Appendix E are **acknowledged with objection**.

### **Alternate Wording:**

The cryptographic system for STAR-Vote will EITHER meet all requirements of Appendix E OR meet a similarly inclusive set of requirements to be drafted for a mix-net-based cryptography solution.

### **Implementation Approach:**

N/A

### **Justification:**

The STAR-Vote system is one variation of a class of electronic voting systems consisting of:

- a submission scheme, i.e., a way to form an encrypted vote and submit it,
- a method of recording encrypted votes in a way that makes deletion, addition, or replacement of ciphertexts infeasible in practice, and
- a cryptographic technique to tally the encrypted votes.

Each step of the chain must be executed in a verifiable way.

One of the advantages of STAR-Vote is that it shares the overall structure of several other electronic voting systems. There is an overwhelming consensus within the cryptographic research community that this is a mature and sound approach. Moreover, it allows each of the components listed above to be adapted to different settings without changing the rest; for example, student union elections, which have less demanding security requirements, may use an Internet-based submission scheme.

In the original STAR-Vote JETS paper and this RFP, so-called homomorphic tallying is used to tally the result and an optimistic mix-net is proposed in one variation to be used to strengthen the assurance in the tallying.

Homomorphic tallying is based on a special property of the cryptosystem that allows multiplying ciphertexts to form a single ciphertext that contains the sum of the votes encrypted in the original ciphertexts. Tallying with a mix-net is more straightforward from a conceptual point of view. It simply decrypts each encrypted vote and outputs the votes in random order. Both functionalities are implemented by a set of servers to distribute the trust needed for privacy. We briefly summarize the pros and cons of each approach below.

When using homomorphic tallying, there is an absolute requirement that each vote is formed correctly. To see this, note that in an election with two candidates encoded as zero and one (to be added homomorphically) a voter could otherwise encrypt a larger integer and effectively submit multiple votes for the candidate encoded as one. Thus, a so-called zero knowledge proof is used to ensure that each ciphertext is formed correctly. A single incorrectly formed ciphertext can change the final tally, or prevent the computation of any tally. Also, a special protocol is needed to handle write-in votes.

Mix-nets are more powerful in that any message can be encrypted, which means that write-in votes are encrypted the same way as any other vote. A zero-knowledge proof is still required, but it is less complex and the same proof can be used for any election. The same zero knowledge proof used for homomorphic tallying can also be used, and is used in cases where one wishes to avoid certain types of coercion. However, in the description of the STAR-Vote system it is argued that protection against coercion using cryptographic means only prevents one of several attack vectors for coercion. Under this assumption, the simpler proof suffices.

Another advantage of a mix-net is that, without any added work, it handles bundled elections, i.e., those where voters express their preferences on candidates for seats as well as binding, or non-binding, referenda.

Thus, we argue that mix-nets are more flexible and powerful tools for tallying that can handle all types of elections, as well as virtually any type of election in the future, with simple configuration that requires no additional advanced security analysis.

An additional output of each type of tallying is a zero-knowledge proof that allows any external party with modest programming skills to implement an algorithm that verifies that the tallying was done correctly.

The main advantage of homomorphic tallying is that its zero-knowledge proof is relatively simple compared to the corresponding zero knowledge proof for the correctness of a mix-net. This makes it somewhat easier to understand, and makes implementing a verifier less demanding.

However, real world experience shows that undergraduates in computer science can independently, and without access to the source code of the mix-net, implement the verification algorithm needed for mix-nets solely from a rigorous description akin to a standards document. For example, the original version of the verifier used for the 2013 municipal elections in Norway was implemented independently by an undergraduate from KTH Royal Institute of Technology.

Thus, the difference between the approaches in this respect is quantitative and not qualitative, and verifiers can be re-used, possibly with minor modifications, for multiple elections.

Homomorphic tallying is also much faster than tallying with a mix-net, but for most practical purposes, a properly implemented mix-net is fast enough. Concrete benchmarks for the Verificatum Mix-Net can be found at the Verificatum AB website.<sup>12</sup>

A mix-net can be used directly for key generation and decryption even if homomorphic tallying is used. Thus, homomorphic tallying can be thought of as a special purpose protocol for settings with a small number of fixed candidates, no write-ins, and stringent requirements on speed and ease of implementing a verifier.

The Verificatum Mix-Net provides all the functionality needed, is fully documented in code and manuals, is thoroughly tested and analyzed, and has a comprehensive benchmark suite that allows prediction of its real world running time.

---

<sup>12</sup> <http://www.verificatum.com/>

The specification of the zero-knowledge proof is rigorous yet concrete, i.e., like standards documents published by NIST it is specified at a byte level. It is mature and has been used by undergraduates at Tel Aviv University and KTH Royal Institute of Technology to implement verifiers using only the specification and example proofs with no access to the source code. This is arguably a requirement for real-world verifiable voting systems.

Due to the number of configuration options and the number of intermediate results, printing test vectors is impractical. Instead the reference implementation can be instrumented to print any relevant values. This greatly simplifies debugging of independently implemented verifiers.

The mix-net has been used to tally more than one million votes in binding elections in Norway, Spain, and Israel, in student, primary, mayoral, and municipal elections.

The software and all additional documentation are available at the Verificatum AB website, as well as via Free & Fair's GitHub organization.<sup>13</sup> It is free for pure research and free for evaluation purposes, it can be used for free by a third party to verify an election, and the license allows modifying the software, posting modified software in any way, and using any modified software. License fees are paid only once (exclusively for running public elections) regardless of whether the original or a modified version is used. Thus, users can effectively act as if the software was released under an open source license after all license fees have been paid.

The Verificatum Mix-Net is the most mature and secure mix-net available today. Using it as the basis of the STAR-Vote Mix-Net Protocol will decrease the amount of development time necessary, and thus free resources to refine specifications, analyze, and implement the rest of the protocol in the most secure way possible. This protocol would also be a more flexible and future-proof solution for Travis County.

## 13 RFP Appendix F: Hardware Requirements

All requirements of Appendix F not mentioned in this section are **acknowledged**. We will use best practices to meet these requirements, but there are likely unknowns that will be discovered throughout development of the COTS hardware solutions and the selected hardware. We will communicate any issues to Travis County as early as possible.

### *10.1 Areas Where Equipment and Devices are Required*

The following equipment and devices are necessary for various aspects of the system. They are enumerated with specific models and availability in our COTS Hardware Recommendations in Section 4.3.2. We list the equipment here in generic terms, since it is not clear which specific models will be available when the time comes to purchase and configure thousands of STAR-Vote devices for the County.

**Operation of Modules.** A PC with standard accessories is all that is necessary for most support modules. As discussed in Section 4.15, a set of SD card readers and SD cards is also necessary for initializing the In-Person Voting Devices.

---

<sup>13</sup> <https://github.com/FreeAndFair/>

**Early Voting and Election Day Polling Locations.** A PC with a Trusted Platform Module, a large touchscreen display, a thermal printer, and a UPS are the necessary core components of the Ballot Control Station and the Voting Station. The interim Ballot Box/Scanner needs a standard (non-digital) ballot box, a microcontroller in a case with an attached small display, and a hand-held 1D barcode scanner. Each device needs a flat surface, access to power, some form of physical security, and a privacy screen. The Audio Ballot Reader needs a small tablet, headphones, and a secure mounting device. The polling place network equipment consists of an appropriate number of network switches, Ethernet cables, and a UPS per switch. Our designed Element B system, of course, needs the *STAR-Vote Enclosure* as well. Likewise, the ground-up design for Element C we have proposed needs its custom Ballot Box/Scanner.

**Ballot-by-Mail.** N/A, as we are not bidding on Element A.

**Storage and Transportation.** We expect that COTS secure storage equipment, such as the Hermitshell EVA protective travel case, will be used for the compute node and UPS. Any equipment we design specifically for STAR-Vote will respect Travis County's needs for efficient storage and transportation.

Note the features shown in design sketches in Figure 4 through Figure 7, including built-in protective covers, the ability to nest devices in storage, and more. Equipment can be stacked on metal shelving, stored in secure lockers, etc. No special storage arrangements are necessary.

As discussed below (under 10.3), the equipment necessary for secure and space-efficient transport is straightforward. COTS system components are small and robust enough that many can be simultaneously transported in the trunk of a car or in a moving van using standard straps and moving blankets. Large numbers of systems can be secured to pallets and moved by truck.

**Other Administrative Requirements.** No other equipment is necessary.

Because our implementation will operate properly on any hardware that fulfills our (precisely stated) assumptions on hardware, no additional class of equipment or devices other than those enumerated above is necessary to operate our STAR-Vote In-Person Voting System or Ballot Box/Scanner.

### *10.3 Plan for the Storage, Transportation, Handling, and Maintenance of Hardware*

Industrial design for Elements B and C systems will be informed, in part, by the needs of Travis County with regards to storage, transportation, handling, and maintenance. We view Travis County's desires and constraints, which we presume mirror those that we have seen from other organizations with which we have worked over the years, as requirements on our industrial design work. Consequently, the prototyping and evaluation cycle that we have planned for the first year of the project includes a multi-stakeholder assessment in these areas. As such, the answers that we provide below on these matters are our thoughts at the moment, given the direction we are heading in our industrial design work.



### *10.3.1 How equipment is to be stored, transported, handled, and maintained*

Our goal is to design in-person voting systems and ballot box/scanner systems to be:

- stored in a space-efficient fashion (i.e., stackable, rather than linear storage);
- robust to abnormal transport conditions (i.e., systems will be robust to environmental conditions, such as those that might be experienced in the back of a pickup truck on a poorly serviced road);
- easily handled by all election officials (i.e., systems must be light enough to be unpacked, configured, and packed by elderly election volunteers); and
- maintained by novices in election technology (i.e., no knowledge of the details of the systems' design or implementation should be necessary to replace a hardware component or to configure and run an election).

These requirements lead us, at present, to focus on a modular *STAR-Vote Enclosure* (discussed in Section 4.3.4) that is both secure and easy to maintain for non-experts, that has a physical robustness commensurate with military enclosures for computing devices (so as to deal well with physical shocks and unpleasant environmental conditions), that has intelligently-chosen materials that are both lightweight and attractive (both in terms of the *STAR-Vote Enclosure* itself and its COTS subcomponents), and that stacks in a secure, LEGO-like fashion.

### *10.3.2 Special containers or transport tools that can be used to ensure equipment is secure from damage*

We do not expect that any special containers or transport tools will be necessary to ensure equipment is secure from damage. Standard moving practices, like secure pallets with blanket wraps, should be sufficient to keep our STAR-Vote systems safe from harm during transport.

### *10.3.3 Devices or physical arrangements that can be used to operate software and data image distribution and archiving*

As discussed elsewhere, our goal is a system that must be lightweight, robust to dynamic and static environmental conditions, and physically and digitally secure. Some of these requirements constrain our design choices during industrial design, prototyping, and design-for-manufacturing (e.g., materials choices). Others imply that we must use specific kinds of compute devices, like the particular Intel NUC we recommend, or data storage devices, such as off-the-shelf SD cards.

In our current design, in order to efficiently certify, configure, and perform L&A tests of the election system for a specific election, we must image at least one SD card per polling place and install one SD card per system. As such, the necessary devices and physical arrangements are quite minimal; a single laptop with an SD card reader would be sufficient to perform all of the certification, configuration, and distribution of digital artifacts necessary to run an entire election in just a few hours of work. That pre-election configuration work could also be parallelized across multiple machines or multiple SD card readers, such as COTS multi-bay SD card readers available from multiple sources for under \$50.

#### 10.3.4 Securely storing equipment at polling locations

Keeping election equipment secure is important before, during, and after an election. COTS equipment is very difficult to secure against manual tampering, theft, and abuse even in well-ordered environments like university labs. Traditional Kensington locks and cables have a role here, as does the use of physical or digital modifications to COTS hardware to disable unused ports and prevent unauthorized interactions.

Designed hardware, such as our proposed *STAR-Vote Enclosure*, opens up new possibilities for preventing unauthorized access to equipment during the various phases of the electoral process. Our hardware security experts, working in tandem with our industrial design team, have many ideas for secure storage, some of which reflect design work already accomplished in Design SHIFT's ORWL physically secure computer.<sup>14</sup> As such, we believe that a designed alternative that uses COTS subcomponents can be made significantly more secure than a plain COTS solution.

## 14 RFP Appendix G: Procedures, Manuals, Instructions, and Training

All requirements of Appendix G are **acknowledged**.

## 15 RFP Appendix H: Data Specifications

### 15.1 Election Definition File (4.1, 5.1, 5.12, 6.0)

We originally created this schema for use in one of our demonstrators. For use in the STAR-Vote system, this file specification would need to be augmented to include references to image and sound files to represent the candidates/issues.

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "title": "Ballot Definition",
  "description": "Definition of a single ballot style",
  "type": "object",
  "properties": {
    "races": {
      "description": "The races/issues on the ballot",
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "text": {
            "description": "The text that should appear for this race/issue on the ballot",
            "type": "string"
          },
          "selections": {
            "description": "A selection for the race/issue",
            "type": "array",
            "items": {
              "type": "string"
            }
          }
        }
      }
    }
  }
}
```

<sup>14</sup> <http://www.orwl.org/>

## 15.2 Tabulator Import File

We originally created this schema for use in one of our demonstrators. The tabulator in this demonstrator assumes that it will only import ballots that should be counted. The STAR-Vote tabulator, however, receives all ballots and must decide which of these to count. With this in mind, the final version of this schema will need to be extended with more information about each ballot. In particular, we will need to know if the ballot box accepted a given ballot and if it is a provisional/accepted ballot.

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "title": "Plurality Election",
  "description": "A single plurality race",
  "type": "object",
  "properties": {
    "isTest": {
      "description": "Value that is always true if it exists, could later be used to
        specify some useful info about the test",
      "type": "boolean",
      "enum": [true]
    },
    "counts": {
      "description": "In a test, this array specifies how many of each of the ballots
        in votes will appear. Can be used for a compressed form of tests",
      "type": "array",
      "items": {
        "type": "integer"
      }
    },
    "votes": {
      "description": "all of the votes in the election",
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "id": {
            "description": "A unique identifier for each
              ballot",
            "type": "integer"
          },
          "selection": {
            "description": "The candidate selected on this
              ballot",
            "type": "integer"
          }
        },
        "required": [
          "id",
          "selection"
        ],
        "additionalProperties": false
      }
    },
    "tiebreak": {
      "description": "the candidate that should be chosen in the event of a tie",
      "type": "integer"
    },
    "results": {
      "description": "a record of what happened as the election was tabulated",
      "type": "object",
      "properties": {
        "winner": {
          "description": "which candidate won the election",
          "type": "integer"
        },
        "tabulation": {
          "type": "array",

```

```

        "items": {
          "type": "object",
          "properties": {
            "candidate": {
              "type": "integer"
            },
            "votes": {
              "type": "integer"
            }
          },
          "required": ["candidate", "votes"],
          "additionalProperties": false
        }
      },
      "required": ["winner"],
      "additionalProperties": false
    }
  },
  "additionalProperties" : false,
  "dependencies" : {
    "isTest" : ["results", "tiebreak", "counts"]
  }
}

```

### 15.3 Tabulator Export File

Because of the simplicity of our Tabulator demonstrator, we have had no previous need for a tabulator export file. The STAR-Vote system, however, will require the export of the homomorphic tally, the NIZK proof of the correctness of the mix, and a record of which ballots the tabulator decided to count and why.

### 15.4 BB/S Export File for Input to Backup & Archiving (5.14)

This file should contain a list of pages that the ballot scanner believes have passed through to the ballot box. For the sake of record keeping we will include additional information such as the number of ballots rejected and why they were rejected.

## 16 Proposal Appendix 1: Project Storytelling

If successful, STAR-Vote will transform how we vote in this country in precisely the right way at an undeniably crucial time. It will place the power of elections in the hands of the people, and the story behind its development must be effectively told. This, as much as anything, will attract potential partners to the *STAR-Vote Entity* outlined in the recent Statement of Intent addendum to this RFP. A powerful, interactive story unfolding in real time could inform and attract not only other election jurisdictions and technology companies, but also foundations and private investors.

One part of the story that we can tell is how an open system can be provably secure, when traditional election vendors rely on precisely the opposite approach. There are non-intuitive aspects to the open source approach that, unless explained correctly and understandably, could face tough opposition in a world where trust in things like ‘science’ and ‘facts’ seems to be wavering. Another aspect that needs effective storytelling is how something as simple as a risk limiting audit can be such a powerful tool to check election results.

The STAR-Vote project is such a paradigm shift that it could be likened to a new mission to the moon. The world will be watching on the first Election Day when citizens cast their votes on machines that are transparent and trustworthy, which cost a fraction of the old, untrustworthy ones they've replaced. That is the story we want to tell.

The following are some of our ideas about how to tell the story on a number of fronts. We suggest that we can produce several artifacts with Travis County during the course of the STAR-Vote project: the *STAR-Vote Blog*, *STAR-Vote Live Feeds*, the *STAR-Vote Book*, and *STAR-Vote Short Films*. These “above and beyond” artifacts will complement those that we discuss elsewhere in this proposal, such as the system’s specification, implementation, and assurance case, the project’s Open Source presence via a GitHub Organization, and the project’s public presence via a *STAR-Vote Website* whose audience is the Travis County voter and, over time, entities and individuals interested in the future of STAR-Vote.

**The STAR-Vote Blog.** Open Source projects that engage with a technical audience and gain a following and contributors often have a blog. Successful blogs, like those written by employees of technology companies such as Microsoft and Valve, permit team members to update the public about their day-to-day goals, work, research, and learnings on a project. While some articles written for the blog will be exclusive to it, most articles will be snapshots of artifacts created for the system’s development, the Book, and the Films (see below). The STAR-Vote project is well-suited to such a continuous stream of quality information, and a blog builds a public, running record of transparency, especially about the technical, social, and political challenges of creating such a system.

**STAR-Vote Live Feeds.** Modern elections offices often have a live video feed of the rooms in which ballots are centrally processed in order to provide transparency and boost voter confidence in an election’s outcome. Moreover, citizens are welcome to observe elections, both in polling places and in county offices, in order to ensure that their outcomes are trustworthy. We believe that this level of transparency is both appropriate and welcome for the development of the STAR-Vote system.

We suggest a reasonable (privacy-preserving, for our employees) “live feed” of our work in several forms: a public dashboard of development progress, a live video feed of one room in our organization in which decision-making happens, a Twitter account that interactively and automatically tweets the activities of the project and its team members to the public, a “comments enabled” link to publicly shared Google documents, and a live chat forum in which team members and the public can interact on a regular basis.<sup>15</sup>

**The STAR-Vote Book.** The *STAR-Vote Book* will include a comprehensive history of the project, from first conception through creation, and will illustrate why STAR-Vote represents such a radical shift in the elections world. It will contain two main parts. Part One—whose audience is the lay public—will tell the story of the people involved with the project and the new and innovative technologies and methods they bring to the table. Part Two—whose audience is the technically-inclined—will contain the literate STAR-Vote system. As such, it will contain the technical specifications, implementations, and evidence of the system’s correctness and security in a Literate Programming style.<sup>16</sup>

**STAR-Vote Short Films.** We can also produce short films, much like we have already done at Free & Fair and for the Elections Verification Network, about the STAR-Vote project—the *STAR-Vote Short Film Series*. An important first short film is a comprehensive history of the project, from first conception through creation. Short films will also include interviews with STAR-Vote team members and visual explanations of key components of STAR-Vote, like its use of end-to-end verifiable cryptography and the effectiveness and importance of risk limiting audits.

---

<sup>15</sup> This could be an IRC, Slack, or Reddit channel—the details are to be determined with Travis County.

<sup>16</sup> This would be like Donald Knuth’s work on TeX, but in a modern context with a Correct-by-Construction approach, similar to Benjamin Pierce et al.’s *Software Foundations* book series (which is now a part of the DeepSpec project, of which Free & Fair is a key industrial partner). See <https://www.cis.upenn.edu/~bcpierce/sf/> and <http://deepspec.org/>.



## 17 Proposal Appendix 2: Bios of Selected Team Members

### 17.1 Dr. Joseph Kiniry

Dr. Joseph Kiniry, Ph.D., is Chief Scientist and CEO of Free & Fair. Prior to working for Free & Fair, Dr. Kiniry provided commercial and public consultancy services to several governments on matters relating to elections, their technology, security, processes, and verifiability. He has worked on election systems for thirteen years; has audited the security, correctness, and reliability of numerous physical and Internet-based voting systems; has developed high-assurance prototypes and products of several election technologies (including, but not limited to, tallying, auditing, voting, ballot marking, and e-poll book (EPB) systems); and sits on the Board of Advisors of the main verifiable elections nonprofit, Verified Voting.

Dr. Kiniry has formally advised four governments (the USA, The Netherlands, the Republic of Ireland, and Denmark) on matters relating to digital elections and has testified before two parliaments. He has also provided informal input and advice to the governments of Norway, Estonia, and the United States. He co-founded and co-ran a multi-year research project on digital elections (the DemTech project<sup>17</sup>) and has supervised numerous BSc, MSc, and PhD theses focusing on elections technologies. His research group has developed several high-assurance peer-reviewed election software systems, including a tally system used in binding European elections for The Netherlands and an EPB system for in Danish national elections. Dr. Kiniry has served as a Principal Investigator on teams for the European Union Council, various DoD branches, the National Science Foundation, and several national funding agencies in Ireland, The Netherlands, and Denmark.

Dr. Kiniry also regularly interacts with and provides input to federal agencies related to elections including the EAC, NIST, and FVAP, and several elections-related non-profits including the OSET Foundation, Common Cause, Democracy Works, the Overseas Vote Foundation, and U.S. Vote. He is a key actor in the newly formed NIST-EAC Public Working Groups.

### 17.2 Dr. Daniel Zimmerman

Dr. Daniel Zimmerman, Ph.D., Chief Architect at Free & Fair, has extensive experience in formal methods, high-assurance software engineering, concurrent and distributed systems, and foundations of computer science. He taught computer science at multiple universities for over a decade, and has contributed to the design and development of several widely used software engineering and formal methods tools. In industry, Dr. Zimmerman has worked primarily in the areas of rigorous software engineering and verifiable elections technology. He is a member of the Elections Verification Network and a contributor in the NIST-EAC Public Working Groups.

### 17.3 Dr. David Cok

Dr. David Cok, Ph.D., will contribute to the project as an expert in software verification systems and in transitioning research ideas into practical software tools. At Eastman Kodak, he was a senior researcher with many patents to his credit, led scientific research labs, and led development groups that implemented novel image processing algorithms in commercial products. Over the past 20 years, he has also developed systems for formal verification of software, both as open source tools and in support of U.S. government research contracts. In

---

<sup>17</sup> <http://demtech.dk/>

particular, he brings expertise in the translation of current programming languages (such as Java, C, LLVM) to logical representations and in applying logical tools, such as automated SMT solvers, that can verify assertions about practical programs. Dr. Cok has served as Principal Investigator on teams for NASA, various DoD branches, and the National Science Foundation.

#### 17.4 Dr. Joey Dodds

Dr. Joey Dodds, Ph.D., will be a key performer in the implementation and verification of STAR-Vote. He recently received his Ph.D. from Princeton University, where he researched proving correctness of C programs including cryptographic algorithms. At Free & Fair, Dr. Dodds has implemented both a tabulator and a risk limiting audit system and done specifications for both. He also fully proved the correctness of the tabulator. He is a key participant in the verification of Amazon's s2n library. He has been responsible for both the verification of the library and implementing a system to automatically report metrics about the progress of the project to Amazon's upper management.

#### 17.5 Dr. Stephanie Singer

Dr. Stephanie Singer, Ph.D., has dual expertise in technology and elections. She studied computer science at Stanford University, earned a Ph.D. in Mathematics from New York University, held a tenured professorship at Haverford College, and worked in the private sector as a data strategist and technology manager. She has extensive experience with elections over more than a decade in roles ranging from poll worker to candidate to election data analyst to Chair of the Philadelphia County (Pennsylvania) Board of Elections. She served four years as elected City Commissioner in Philadelphia. For three years, she served on the Board of the County Commissioners Association of Pennsylvania and as Co-Chair of the statewide Elections Reform Committee of that organization.

#### 17.6 Dr. Douglas Wikström (Verificatum AB)

Dr. Douglas Wikström, Ph.D., is an associate professor in cryptography at KTH Royal Institute of Technology. He researches theoretical cryptography, but ever since 2000 he has spent part of his time on cryptographic aspects of electronic voting systems and his thesis focused on mix-nets. Today he is considered to be a world-leading expert on this topic.

He founded the company Verificatum AB in 2011 to refine the mix-net implementation he completed 2008 into an industrial grade product. He invented key mix-net components that have since been adopted in the Helios and the UniVote voting systems, but he has also discovered several practical attacks and vulnerabilities of mix-nets proposed in the literature, e.g., Civitas, a version of Scantegrity, and the scheme provided by Scytl to Norway 2011.

He has co-chaired the EVOTE conference and served on several program committees of conferences in the field, and he has served as an expert at hearings of Swedish government committees as well as the Swedish Voting Authority multiple times. He is a member of the Election Verification Network (EVN).

### 17.7 Drew Davies (Oxide Design Co.)

Oxide Design Co. is a branding and design firm established in 2001. During the past 15 years, Oxide's work has been awarded by every major design competition, including One Show Design, the CLIO Awards, and six different times by *Communication Arts Design Annual*. Oxide's clients range from one-person startups to Fortune 200 companies, across a multitude of industries. Their work spans the consumer/retail, business-to-business, and public/civic design spaces.

Because Oxide believes very strongly in the power of design to create progressive change, over 50 percent of Oxide's work is donated — in whole or in part — to a wide range of non-profit and charitable organizations.

Oxide is heavily active in the national civic design space, working regularly with states, counties, and federal government agencies, including New York State Board of Elections, California Secretary of State, Virginia Board of Elections, and Pennsylvania Department of State. Oxide worked with the Federal Voting Assistance Program (FVAP) to redesign both the online and print versions of the Federal Post Card Application (FPCA) and Federal Write-in Absentee Ballot (FWAB), as well as the Voting Assistance Guide, for overseas voters. In addition, Oxide served as part of the core design and research team that developed the U.S. Election Assistance Commission's national ballot design standards, and subsequently helped develop the Field Guides to Ensuring Voter Intent — pocket-sized guides containing field-researched, critical election design techniques that help ensure that every vote is cast as voters intend.

One of Oxide's most notable contributions in civic design is developing the Anywhere Ballot — an online ballot marking interface — in partnership with the Center for Civic Design and the University of Baltimore. The project created a thoroughly tested, highly usable tool allowing U.S. military and overseas citizens — as well as persons with physical or cognitive disabilities — to vote more easily. Anywhere Ballot's ultimate goal is to allow every citizen to vote on any device, anywhere, at any time.

### 17.8 Morgan Miller (Morgan Miller UX)

Morgan Miller is an experienced User Experience (UX) professional with a deep background in scientific research. She is currently a User Experience Architect for Morgan Miller UX, LLC, where she leads teams through a UX discovery, architecture, and research process; designs and executes research studies; synthesizes research data to create actionable recommendations; and builds information architecture including taxonomy, sitemaps, and wireframes. She has done work for Overseas Vote Foundation, Intel, Mozilla Foundation, BMC Software, Esri, World Wildlife Fund, Nike, Moda, Providence Health, and Cambia Health. She earned a B.A. in Mathematics from Reed College and an M.S. in Computer Science from the University of Lugano, Switzerland, where she was a cryptography researcher.

### 17.9 Jon Levy (AMA Studios)

Jon Levy is an Emmy Award-Winning Design Director with two decades of experience delivering projects for Fortune 100 firms including Activision, Sony, Nike, MIT, US Army, ABC, Warner Bros, and Disney. He has organized creative teams across international locations, including the Philippines, India and Brazil. His extensive portfolio includes Industrial Design, Environmental Design, Visualization, and Interactive development. In addition to being the Director of AMA Studios, Jon is the Manager of the NASA Advanced Concepts Laboratory. The ACL is a digital creation studio located on the Langley Research Center. The ACL is in the unique position of participating in a wide array of early stage NASA projects. The ACL gives form to technologies, projects and programs by clarifying the design and communicating the story.

### 17.10 Harri Hursti (Nordic Innovation Labs)

Harri Hursti is one of the world's foremost experts on the topic of electronic voting security, having served in all aspects of the industry sector. He is an authority on uncovering critical problems in electronic voting systems worldwide, including in the U.S., Finland, Estonia, the Philippines, and Argentina. As a consultant, he has conducted and co-authored many studies, both academic and commercial, on numerous election systems' data security and vulnerabilities. These studies have come at the request of officials, legislators and policy makers in 5 countries; including the U.S. government, at both the state and federal level. Mr. Hursti is famously known for his successful attempt to demonstrate how the Diebold Election Systems' voting machines could be hacked, ultimately altering final voting results. Hursti performed two voting machine hacking tests which became widely known as the *Hursti Hacks*. The Hursti Hack tests were filmed and turned into an acclaimed HBO documentary called *Hacking Democracy* which was nominated for an Emmy award for outstanding investigative journalism. Mr. Hursti received the EFFI Winston Smith Award in 2008 and the EFF Pioneer Award in 2009 for his work in election security.

### 17.11 Maggie MacAlpine (Nordic Innovation Labs)

Margaret "Maggie" MacAlpine is an election auditing specialist and system testing technologist who has worked on a variety of projects that include electronic testing of voting registration systems, election security and election fraud. Highly specialized technologist in testing and performing risk limiting and transitive audits on election results, she has consulted on multiple projects in Florida, Connecticut, and Colorado. She has served as an advisor for the office of the Secretary of State of California for the Risk Limiting Audit Pilot Program 2011-2012, and is widely regarded as an expert on the use of high-speed scanners for conducting post-election audits. Ms. MacAlpine was a contributing researcher on the "Security Analysis of the Estonian Internet Voting System" in partnership with the University of Michigan.

### 17.12 Stefan Carpentier

Stefan Carpentier delivered successful engineering management in a variety of fields including Consumer Electronic Design, Semiconductor Design, Software Design and MEMs Design. Development in close cooperation with the customer, on time, on/under budget, on target. Working with people and building fair, innovative, beautiful products is what makes him "tick".

**17.13 Daniel Nelson**

Daniel Nelson specializes in software test methodology and navigating the complexities of legal conformance, platform supplier approval, and wireless network operator approval. He has deep expertise in multiple categories of consumer electronics including tablets, smartphones, GPS Navigation devices, and handheld/pocket organizers on multiple software platforms including Microsoft Windows CE (and Windows Mobile), Symbian (UIQ and Series 60), Linux, and Google Android. Daniel is currently engaged in the validation and compliance activities surrounding Android-based tablets and other CE products. He was previously the Validation Manager for TomTom Inc. covering all testing (hardware and regional software variance), compliance, and approvals activities in North and South America. Positions prior to TomTom include Validation Manager for Symbian Smartphone Development at Motorola, and Test and Automation Lead at Sendo.

**17.14 Michael Kiniry**

Michael Kiniry, Communicator at Free & Fair, is a media expert with backgrounds in radio, print, and photojournalism. He spent nearly a decade as a public radio reporter, producer, and host and has been a freelance photographer and writer for the past 14 years. Mike is also a videographer and editor and is the EVN's dedicated videographer/producer.

**Cost Proposal/Schedule of Items**

Per RFP instructions, one original hard copy was submitted in a sealed envelope separate from this proposal. An electronic version was included on flash drive submission, saved as a separate file entitled “Attachment 11 Schedule of Items.pdf.”



## Proposer References

The following tables list references for Elements B and C for which we have provided similar goods or services within the last five years. (Also refer to Qualifications Questionnaire, Item 12.)

**Element B, Table 4: Project Reference #1**

<b>Location:</b> Washington, DC		<b>Date(s) of Work:</b> Mar 2015 – Sep 2016
<b>Description of Goods and Services:</b> <i>Private Elections Quality and Security Audits.</i> Within this project, Free & Fair principals performed a quality and security audit of an Internet Voting system used by most unions in the USA, and also provided expert input into national policy in union elections.		
<b>Reference Contact Information:</b>		
Company Name:	US Department of Labor	
Contact Full Name:	Leonard Tambra	
Contact Mailing Address:	200 Constitution Avenue NW, Suite N-2474 Washington DC 20210	
Contact Email Address:	leonard.tambra@dol.gov	
Contact Telephone Number	(202) 693-5744	

**Element B, Table 4: Project Reference #2**

<b>Location:</b> Portland, OR		<b>Date(s) of Work:</b> Nov 2015 – Mar 2016
<b>Description of Goods and Services:</b> <i>C11 Verification Technology.</i> Within this project, Free & Fair principals created formal verification technology for the National Institute of Standards and Technology (NIST). This technology focuses on verifying properties of modern C code, which uses new keywords to enable developers to specify the use of novel memory models for modern multi-core systems.		
<b>Reference Contact Information:</b>		
Company Name:	National Institute of Standards and Technology (NIST)	
Contact Full Name:	Paul Black	
Contact Mailing Address:	100 Bureau Drive, Stop 8970	

	Gaithersburg, MD 20899-8970
Contact Email Address:	paul.black@nist.gov
Contact Telephone Number	(301) 975-4794

**Element B, Table 4: Project Reference #3**

<b>Location:</b> Portland, OR		<b>Date(s) of Work:</b> Mar 2015 – Oct 2016
<b>Description of Goods and Services:</b> <i><b>Galois Ultra Low Power High Assurance Asynchronous Cryptography.</b></i> Within this project, Free & Fair principals invented the Galois Ultra Low Power High Assurance Asynchronous Cryptography (GULPHAAC) chip, which represents an entirely new technology for the automatic generation of hardware designs for chip (ASIC) fabrication. The demonstration system that we built is the world's first formally verified cryptography chip, and is also the world's first asynchronous (clockless) crypto chip. The chip operates at threshold voltage; it is therefore extremely low power and low energy, and is energy-competitive with the lowest energy devices ever invented. The chip is power invariant—if provided more voltage it runs faster—and is consequently speed competitive with the best chips on the market. Finally, the chip has an assurance case far in excess of any crypto chip on the market.		
<b>Reference Contact Information:</b>		
Contact Full Name:	Bryan Weeks	
Contact Mailing Address:	9800 Savage Road, Suite 6845 Fort Meade MD 20755-6845	
Contact Email Address:	beweeks@tycho.ncsc.mil	
Contact Telephone Number	(443) 634-3936	

**Element C, Table 4: Project Reference #1**

<b>Location:</b> Portland, OR		<b>Date(s) of Work:</b> Mar 2015 – Oct 2016
<b>Description of Goods and Services:</b> <i><b>Galois Ultra Low Power High Assurance Asynchronous Cryptography.</b></i> Within this project, Free & Fair principals invented the Galois Ultra Low Power High Assurance Asynchronous Cryptography (GULPHAAC) chip, which represents an entirely new technology for the automatic generation of hardware designs for chip (ASIC) fabrication. The demonstration system that we built is the world's first formally verified cryptography chip, and is also the world's first asynchronous (clockless) crypto chip. The chip operates at threshold voltage; it is therefore extremely low power and low energy, and is energy-competitive with the lowest energy devices ever invented. The chip is power invariant—if provided more voltage it runs faster—and is consequently speed competitive with the best chips on the market. Finally, the chip has an assurance case far in excess of any crypto chip on the market.		
<b>Reference Contact Information:</b>		
Contact Full Name:	Bryan Weeks	
Contact Mailing Address:	9800 Savage Road, Suite 6845 Fort Meade MD 20755-6845	
Contact Email Address:	beweeks@tycho.ncsc.mil	
Contact Telephone Number	(443) 634-3936	

**Element C, Table 4: Project Reference #2**

<b>Location:</b> Portland, OR		<b>Date(s) of Work:</b> Nov 2015 – Mar 2016
<b>Description of Goods and Services:</b> <i><b>C11 Verification Technology.</b></i> Within this project, Free & Fair principals created formal verification technology for the National Institute of Standards and Technology (NIST). This technology focuses on verifying properties of modern C code, which uses new keywords to enable developers to specify the use of novel memory models for modern multi-core systems.		
<b>Reference Contact Information:</b>		
Company Name:	National Institute of Standards and Technology (NIST)	
Contact Full Name:	Paul Black	

Contact Mailing Address:	100 Bureau Drive, Stop 8970 Gaithersburg, MD 20899-8970
Contact Email Address:	paul.black@nist.gov
Contact Telephone Number	(301) 975-4794

**Element C, Table 4: Project Reference #3**

<b>Location:</b> Portland, OR	<b>Date(s) of Work:</b> Jun 2014 – Jul 2015
<b>Description of Goods and Services:</b> <i>Future of Voting.</i> Within this project, Free & Fair principals led a research study into the feasibility of End-to-End Verifiable Internet Voting (E2E-VIV), and edited and co-authored a 136-page report with several technical appendices that lays out the necessary and sufficient conditions for the realization of such an ambitious but controversial system. This project also necessitated the management of an extremely diverse team of international experts in relevant topics—a team that was at odds internally given the nature of the topic and heated opinions about security, enfranchisement, policy, and more. Some of the technical elements of this project, particularly its informal domain model of elections and core ideas about cryptographic framing of E2E-V systems, are directly relevant to the STAR-Vote project. This report is now the de facto reference for all R&D in internet voting.	
<b>Reference Contact Information:</b>	
Contact Full Name:	Susan Dzieduszycka-Suinat
Contact Mailing Address:	U.S. Vote Foundation 4325 Old Glebe Road Arlington, VA 22207 USA
Contact Email Address:	susan@usvotefoundation.org
Contact Telephone Number	+49 (0) 89 64939133

**Element C, Table 4: Project Reference #4**

<b>Location:</b> Portland, OR		<b>Date(s) of Work:</b> Sept 2014 – present
<b>Description of Goods and Services:</b> <p><i><b>SHAVE.</b></i> The goal of SHAVE is to inform about, and assess the feasibility of, a practical end-to-end assurance case for mission critical systems that run on COTS and bespoke hardware. The SHAVE demonstrator is an inline streaming encryption engine realized on RISC-V, a modern open source processor. Such a device is comparable to the “bump-in-wire” encryption devices deployed today within the Department of Defense, except that it will include a formal assurance case to show that it is perfectly fit for purpose, correct, and secure. It will be realized via a cryptographic extension to RISC-V, a small formally verified firmware layer for interacting with that extension, and a lightweight API atop the firmware layer to make it accessible to programming languages like C and Rust. Within SHAVE we also are producing the SHAVE formal method for building the aforementioned end-to-end assurance case.</p>		
<b>Reference Contact Information:</b>		
Contact Full Name:	Linton Salmon (Program Manager) and Marnie Dunsmore (SETA)	
Contact Mailing Address:	DARPA 675 N Randolph St Arlington, VA 22203	
Contact Email Address:	linton.salmon@darpa.mil marnie.dunsmore.ctr@darpa.mil	
Contact Telephone Number	(703) 526-2886 ext. 2886	

## **Description of Proposer**

Free & Fair was established in 2015 as a division of Galois, Inc., a privately held U.S.-owned and -operated corporation established in 1999 in Portland, Oregon. We are headquartered in Portland with an office in Arlington, VA and currently have 65 employees. Our Portland headquarters, where this proposed work will be done, is located in a 20,472-square-foot office space in the Commonwealth Building in downtown. We have an in-house data center and all the necessary IT infrastructure required for our various computer science research and development projects.

Galois specializes in the research and development of new technologies that solve the most difficult problems in computer science. We are passionate about the trustworthiness of critical systems, and work to ensure that systems work as intended, and only as intended. Our team works closely with clients to achieve a balance between the privacy/cost/speed challenges involved in making systems more trustworthy.

We care deeply about real-world use of our R&D efforts and work diligently to transition them into use. Our clients, which are mostly in the U.S. government, derive value working with us as trusted advisors and hold us to high standards for the actual production of algorithms and code that embody our work together.

Key government clients include DARPA, Office of Naval Research, Air Force Research Laboratory, Department of Homeland Security, Intelligence Community, NASA, and NIST.

Additional details such as address, contact information, list of principals, and past firm experience can be found in the attached Qualifications Questionnaire form.



## Description of Typical Engagements

Our core project management principles focus on **Customer Caretaking, Social Contracts, Continuous Improvement, Artifacts and Evidence, and Transparency.**

**Customer Caretaking.** For all projects, we have a dedicated Free & Fair team member whose role is to represent the interests of the client. They are actively engaged with the client and have a role in all project management decisions. They build a deep trust relationship with the client's key performers. This position is a reflection of the trust relationship between us and our clients.

**Social Contracts.** Our systems engineering artifacts capture technical interdependencies among project team members, but the glue that holds the team together and makes the team work well is our collective social contracts. Our performers explicitly discuss and acknowledge client-supplier relationships between team members and always perform to exceed not only the expectations of our external client (e.g., Travis County), but also each internal client (another team member).

**Continuous Improvement.** Social contracts are renegotiated frequently and fluidly and are directly reflected upon immediately upon completion. For example, at the end of a thirty-minute stand-up meeting discussing a milestone that we just reached and what comes next, we often have a five-minute discussion about what worked well and where improvements can be made with regards to that particular piece of work. In particular, we focus on its embedded social contracts. The individuals in our organization always attempt to maximize efficiency, impact, and joy at work.

**Artifacts and Evidence.** We focus on artifacts and evidence in a project or product. “Meta” aspects like processes and checklists serve meaningful outcomes. This focus on the meaningful is pervasive. Principles trump rules. For example, provable security is mandatory; “security theater” is prohibited.

**Transparency.** Finally, whether it is with regard to our technology, business practices, or project management approach, transparency is the core principle by which we operate. Telling each other, and the client, when something is working well or working poorly, early and honestly, is common. If necessary, we will tell a client that a technical direction they are excited about is inappropriate and provide objective evidence to justify that conclusion. We always keep the client informed, whether we are ahead of the game or behind the eight ball. In all aspects, and for all projects, we believe that transparency is the keystone of our operation. Without it, our election systems cannot be trustworthy and will not be successful.

**Proposer Representative**

Below is the list of individuals, along with their contact information, who are responsible for answering technical, functional, and contractual questions with respect to this proposal.

**Technical Point of Contact:**

Dr. Joseph Kiniry  
ph (503) 808-7229  
[kiniry@freeandfair.us](mailto:kiniry@freeandfair.us)

**Functional Point of Contact:**

Anne Marie McClaran  
ph (503) 808-7203  
[annemarie@galois.com](mailto:annemarie@galois.com)

**Contractual Point of Contact:**

Jodee LeRoux  
ph (503) 808-7209  
[jodee@galois.com](mailto:jodee@galois.com)

## **Ethics Affidavit**

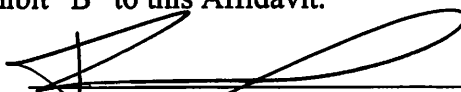
STATE OF TEXAS}  
COUNTY OF TRAVIS}

## ETHICS AFFIDAVIT

Date: 1/23/2017  
Name of Affiant: Jodee Lepoux  
Title of Affiant: General Counsel  
Business Name of Proposer: Baldis, Inc.  
County of Proposer: Multnomah

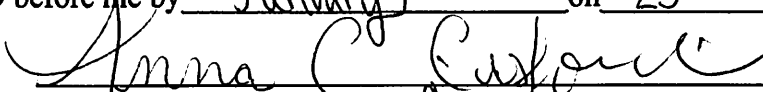
Affiant on oath swears that the following statements are true:

1. Affiant is authorized by Proposer to make this affidavit for Proposer.
2. Affiant is fully aware of the facts stated in this affidavit.
3. Affiant can read the English language.
4. Proposer has received the list of key contracting persons associated with this solicitation which is attached to this affidavit as Exhibit A.
5. Affiant has personally read Exhibit A to this Affidavit.
6. Affiant has no knowledge of any Key Contracting Person on Exhibit "A" with whom Proposer is doing business or has done business during the 365 day period immediately before the date of this affidavit whose name is not disclosed in Exhibit "B" to this Affidavit.

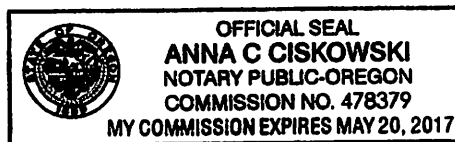
  
\_\_\_\_\_  
Signature of Affiant

421 SW 8th Avenue Suite 300 Portland, OR 97204  
\_\_\_\_\_  
Address

SUBSCRIBED AND SWORN TO before me by January on 23, 2017.

  
\_\_\_\_\_  
Notary Public, State of Oregon

Anna C Ciskowski  
\_\_\_\_\_  
Typed or printed name of notary  
My commission expires: May 20, 2017



**EXHIBIT A**  
**LIST OF KEY CONTRACTING PERSONS**  
September 14, 2016

**CURRENT**

<u>Position Held</u>	<u>Name of Individual Holding Office/Position</u>	<u>Name of Business Individual is Associated</u>
County Judge .....	Sarah Eckhardt	
County Judge (Spouse) .....	Kurt Sauer	Kelly Hart LLP
Chief of Staff.....	Peter Einhorn	
Executive Assistant .....	Loretta Farb	
Executive Assistant.....	Joe Hon	
Executive Assistant.....	Maya Reisman	
Commissioner, Precinct 1 .....	Ron Davis	
Commissioner, Precinct 1 (Spouse).....	Annie Davis	Seton Hospital
Executive Assistant.....	Deone Wilhite	
Executive Assistant.....	Felicitas Chavez	
Executive Assistant.....	Sue Spears	
Commissioner, Precinct 2 .....	Brigid Shea	
Commissioner, Precinct 2 (Spouse).....	John Umphress	Austin Energy
Executive Assistant .....	Barbara Rush	
Executive Assistant .....	Kristian Caballero	
Executive Assistant .....	Melissa Velasquez	
Commissioner, Precinct 3 .....	Gerald Daugherty	
Commissioner, Precinct 3 (Spouse).....	Charyl Daugherty	Consultant
Executive Assistant.....	Bob Moore	
Executive Assistant.....	Martin Zamzow	
Executive Assistant.....	Madison A. Gessner	
Commissioner, Precinct 4 .....	Margaret Gomez	
Executive Assistant.....	Edith Moreida	
Executive Assistant.....	Norma Guerra	
County Treasurer .....	Dolores Ortega-Carter	
County Auditor .....	Nicki Riley	
County Human Resources Interim.....	Todd L. Osburn*	
County Executive, Administrative.....	Vacant	
County Executive, Planning & Budget.....	Jessica Rio	
County Executive, Emergency Services .....	Danny Hobby	
County Executive, Health/Human Services.....	Sherri E. Fleming	
County Executive, TNR .....	Steven M. Manilla, P.E.	
County Executive, Justice & Public Safety .....	Roger Jefferies	
Director, Facilities Management.....	Roger El Khoury, M.S., P.E.	
Chief Information Officer .....	Tanya Acevedo	
Director, Records Mgmt & Communications .....	Steven Broberg	
Travis County Attorney .....	David Escamilla	
First Assistant County Attorney .....	Steve Capelle	
Executive Assistant, County Attorney .....	James Collins	
Director, Land Use Division .....	Tom Nuckols	
Attorney, Land Use Division .....	Julie Joe	
Attorney, Land Use Division .....	Christopher Gilmore	
Director, Transactions Division .....	John Hille	
Attorney, Transactions Division .....	C.J. Brandt*	
Attorney, Transactions Division .....	Ann-Marie Sheely	
Attorney, Transactions Division .....	Barbara Wilson	
Attorney, Transactions Division .....	Jennifer Kraber	
Attorney, Transactions Division .....	Tenley Aldredge	
Director, Health Services Division .....	Beth Devery	
Attorney, Health Services Division .....	Elizabeth Winn	
Attorney, Health Services Division .....	K. Nicole Aquino*	
Attorney, Health Services Division .....	Prema Gregerson	
Attorney, Health Services Division .....	Barbara E. Misle	
Attorney, Health Services Division .....	Ruben Baeza, Jr.	
Attorney, Health Services Division .....	Holly Gummert*	

Purchasing Agent .....	Cyd Grimes, C.P.M., CPPO
Assistant Purchasing Agent .....	Elaine Casas, J.D.
Assistant Purchasing Agent .....	Marvin Brice, CPPB
Assistant Purchasing Agent .....	Bonnie Floyd, CPPO, CPPB
Purchasing Agent Assistant IV .....	CW Bruner, CTP, CPPB
Purchasing Agent Assistant IV .....	Lee Perry
Purchasing Agent Assistant IV .....	Jason Walker
Purchasing Agent Assistant IV .....	Patrick Strittmatter, CPPB
Purchasing Agent Assistant IV .....	Lori Clyde, CPPO, CPPB, CTPE
Purchasing Agent Assistant IV .....	Scott Wilson, CPPB
Purchasing Agent Assistant IV .....	Jorge Talavera, CPPO, CPPB
Purchasing Agent Assistant IV .....	Loren Breland, CPPB
Purchasing Agent Assistant IV .....	John E. Pena, CTPM, CPPB
Purchasing Agent Assistant IV .....	Kimberly Roohms
Purchasing Agent Assistant IV .....	Jonathan Harris*
Purchasing Agent Assistant IV .....	Veronica Frederick*
Purchasing Agent Assistant III .....	Logan Brown, CTCM, CTPM*
Purchasing Agent Assistant III .....	David Walch
Purchasing Agent Assistant III .....	Jean Liburd
Purchasing Agent Assistant III .....	Sydney Ceder
Purchasing Agent Assistant III .....	Ruena Victorino
Purchasing Agent Assistant III .....	Rachel Fishback
Purchasing Agent Assistant II.....	L. Wade Laursen
Purchasing Agent Assistant II.....	Sam Francis
HUB Coordinator.....	Allen J. Roberts, MBA, CTP*
HUB Specialist.....	Betty Chapa
HUB Specialist.....	Jerome Guerrero
HUB Specialist.....	Paula Ann Pitifer
Purchasing Business Analyst .....	Scott Worthington
Purchasing Business Analyst .....	Rosalinda Garcia
County Clerk.....	Dana DeBeauvoir
County Clerk's Office.....	Ron Morgan
County Clerk's Office.....	Scott Flom
County Clerk's Office.....	Candi Semple
County Clerk's Office.....	Michael Winn
County Clerk's Office.....	Geetha Lingham
Consultant/Project Director .....	Neil McClure
Project Consultant.....	Bryce Eakin
Project Consultant.....	Susan Bell
Technical Consultant .....	Dan Wallach, Rice University
Technical Consultant .....	Neil McBurnett
Technical Consultant .....	Olivier Pereria, UC Louvain, Belgium
Technical Consultant .....	Ronald Rivest, MIT
Technical Consultant .....	Josh Benaloh, Microsoft, Inc.
Technical Consultant .....	Mike Byrne, Rice University
Technical Consultant .....	Phil Kortum, Rice University
Technical Consultant .....	Philip Stark, UC-Berkeley
Election Study Group.....	Nan Clayton, Texas League of Women Voters
Election Study Group.....	Alcia DelRio, Austin Community College
Election Study Group.....	Arthur De Bianca, Travis County Libertarian Party
Election Study Group.....	Maria Jimenez, Presiding Judge – Democratic Party
Election Study Group.....	Jannette Goodall, City of Austin
Election Study Group.....	Sherri Greenberg, LBJ School of Public Affairs
Election Study Group.....	Zoe Griffith, Austin ISD
Election Study Group.....	Jim Henson, UT Department of Government
Election Study Group.....	Reuben Leslie, Travis County Democratic Party
Election Study Group.....	Ron Lucey, Austin Mayor's Committee for People with Disabilities
Election Study Group.....	Lorenzo Sadun, UT Department of Mathematics
Election Study Group.....	James Dickey, Chair, Travis County Republican Party
Election Study Group.....	May Schmidt, Early Voting Deputy
Election Study Group.....	Bill Stout, Green Party of Texas
Election Study Group.....	Robert Sheldon, Election Day Judge
Election Study Group.....	Vincent Harding, Chair, Travis County Democratic Party



Election Study Group.....Karen Renick, VoteRescue  
 Election Study Group.....Daniel Biering, Election Judge  
 Election Study Group.....Mike Conwell, Election Judge/Political Activist  
 Election Study Group.....Wilhelmena DeMarco, Former State Representative  
 Election Study Group.....Susan DeMarco  
 Election Study Group.....Jim McNabb, Retired Journalist  
 Election Study Group.....Madeline Perasall, Political Candidate  
 Election Study Group.....Sabine Romero, Attorney, City of Austin

#### FORMER EMPLOYEES

<u>Position Held</u>	<u>Name of Individual Holding Office/Position</u>	<u>Date of Expiration</u>
Attorney, Health Services Division .....	Randy M. Floyd.. .....	10/03/16
Purchasing Agent Assistant IV .....	Richard Villareal .....	10/31/16
Purchasing Agent Assistant III .....	Anthony Webb.... .....	02/05/17
Purchasing Agent Assistant IV .....	Jesse Herrera..... .....	03/04/17
County Human Resources.....	Debbie Maynor... .....	03/17/17
Attorney, Transactions Division .....	Daniel Bradford .. .....	06/01/17
HUB Coordinator.....	Sylvia Lopez..... .....	07/31/17

\* - Identifies employees who have been in that position less than a year.

**EXHIBIT B**

**DISCLOSURE**

**Proposer acknowledges that Proposer is doing business or has done business during the 365-day period immediately prior to the date on which this proposal is due with the following Key Contracting Persons and warrants that these are the only such Key Contracting Persons:**

---

---

---

---

---

---

**If no one is listed above, Proposer warrants that Proposer is not doing business and has not done business during the 365-day period immediately prior to the date on which this proposal is due with any key contracting person.**

## **HUB Program Subcontracting Declaration**

**HISTORICALLY UNDERUTILIZED BUSINESS (HUB) PROGRAM SUBCONTRACTING DECLARATION****SECTION 1 BIDDER AND SOLICITATION INFORMATION**

Bidder Company Name: Galois, Inc., dba Free & Fair		State of Texas VID#:	
Address: 421 SW Sixth Avenue, Ste. 300	City: Portland	State: OR	Zip Code: 97204
Contact: Dr. Joseph Kiniry	Phone No.: 503-626-6616	Fax No.: 503-350-0833	E-mail: <a href="mailto:kiniry@freeandfair.us">kiniry@freeandfair.us</a>
Project Name: STAR-Vote	Total Bid Amount: \$4,816,486	Solicitation #: RFP P1609-008-LC	
Is your company a certified HUB? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No		Indicate Gender & Ethnicity:	
Certifying Agency (Check all applicable):	<input type="checkbox"/> State of Texas (HUB)	<input type="checkbox"/> City of Austin (M/WBE)	<input type="checkbox"/> Texas Unified Certification Program (TUCP) (DBE)

**Definitions:**

HUB – Historically Underutilized Business • M/WBE – Minority/Women-Owned Business Enterprise • DBE – Disadvantage Business Enterprise

The policy of the Travis County Purchasing Office is to ensure a "Good Faith Effort" (GFE) is made to assist certified HUB vendors and contractors in receiving contracts in accordance with the HUB Program policies and the Minority and Woman-owned Business (M/WBE) goals adopted by the Travis County Commissioners Court. Travis County encourages all Bidders to register as a County vendor through the County's online vendor registration.

\*Prime Contractors who are awarded contracts with the County are required to make a "Good Faith Effort" to subcontract with HUBs. This includes professional services associated with the projects.

**SECTION 2 SUBCONTRACTING INTENTIONS**

Percentage to be subcontracted to Certified HUBs:

Total MBE Dollars:	Total MBE Percentage:	Total WBE Dollars:	Total WBE Percentage:
--------------------	-----------------------	--------------------	-----------------------

Check the box that applies to the Bidder:

- ☐ We are able to fulfill all subcontracting opportunities with our own resources. If circumstances necessitate the use of any subs, I agree to seek the timely authorization by the County and adhere to the submission of any required documentation. (Complete Sections 5, 6 and 8)
- ☐ We plan to subcontract some or most of the opportunities of this project and meet or exceed the set goals. (Complete Sections 3, 4, 6 and 8)
- ☒ We plan to utilize subcontractors on this project, but will not meet the set goals. (Complete Sections 3, 4, 5, 6 and 8)

The HUB Program policies and Minority and Woman-Owned Business **subcontracting goals** shall be applicable to the eligible procurement dollars spent in the areas of Construction, Commodities, Services, and Professional Services.

<input type="checkbox"/> <b>COMMODITIES</b>	<b>Overall MBE Goal:</b> 3.5%	<b>Sub-goals:</b> 0.3% African-American 2.5% Hispanic 0.7% Asian/Native-American	<b>Overall WBE Goal:</b> 6.2%
<input type="checkbox"/> <b>CONSTRUCTION</b>	<b>Overall MBE Goal:</b> 13.7%	<b>Sub-goals:</b> 1.7% African-American 9.7% Hispanic 2.3% Asian/Native-American	<b>Overall WBE Goal:</b> 13.8%
<input checked="" type="checkbox"/> <b>SERVICES</b>	<b>Overall MBE Goal:</b> 14.1%	<b>Sub-goals:</b> 2.5% African-American 9.9% Hispanic 1.7% Asian/Native-American	<b>Overall WBE Goal:</b> 15.0%
<input type="checkbox"/> <b>PROFESSIONAL SERVICES</b>	<b>Overall MBE Goal:</b> 15.8%	<b>Sub-goals:</b> 1.9% African-American 9.0% Hispanic 4.9% Asian/Native-American	<b>Overall WBE Goal:</b> 15.8%

**SECTION 3 DISCLOSURE OF CERTIFIED HUB SUBCONTRACTORS**

(Duplicate as necessary)

Travis County exercises the right to verify subcontractors listed on this project. It is the County's practice to consider ethnicity before gender when distinguishing HUB certifications and calculating goal achievement.

*Note: To be considered "certified" with the State of Texas, City of Austin or the Texas Unified Certification Program, please attach a current and valid certificate. Sub-goals are included to assist you in diversifying your subcontractors.*

Sub Company Name: Morgan Miller UX		State of Texas VID#: N/A	
Address: 3402 SE Main Street	City: Portland	State: OR	Zip Code: 97214
Contact: Morgan Miller	Phone No.: <a href="http://morganmillerux.com">http://morganmillerux.com</a>	Fax No.:	E-mail: <a href="mailto:morganmillerux@gmail.com">morganmillerux@gmail.com</a>
Subcontract Amount:	Percentage:	Description of Work: UI/UX Lead, Usable Security in Elections	
Is your company a certified HUB? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	Indicate Gender & Ethnicity: Female Caucasian		
Certifying Agency (Check all applicable):	<input type="checkbox"/> State of Texas (HUB)	<input type="checkbox"/> City of Austin (M/WBE)	<input type="checkbox"/> Texas Unified Certification Program (TUCP) (DBE)

Sub Company Name:		State of Texas VID#:	
Address:	City:	State:	Zip Code:
Contact:	Phone No.:	Fax No.:	E-mail:
Subcontract Amount:	Percentage:	Description of Work:	
Is your company a certified HUB? <input type="checkbox"/> Yes <input type="checkbox"/> No	Indicate Gender & Ethnicity:		
Certifying Agency (Check all applicable):	<input type="checkbox"/> State of Texas (HUB)	<input type="checkbox"/> City of Austin (M/WBE)	<input type="checkbox"/> Texas Unified Certification Program (TUCP) (DBE)

Sub Company Name:		State of Texas VID#:	
Address:	City:	State:	Zip Code:
Contact:	Phone No.:	Fax No.:	E-mail:
Subcontract Amount:	Percentage:	Description of Work:	
Is your company a certified HUB? <input type="checkbox"/> Yes <input type="checkbox"/> No	Indicate Gender & Ethnicity:		
Certifying Agency (Check all applicable):	<input type="checkbox"/> State of Texas (HUB)	<input type="checkbox"/> City of Austin (M/WBE)	<input type="checkbox"/> Texas Unified Certification Program (TUCP) (DBE)

Sub Company Name:		State of Texas VID#:	
Address:	City:	State:	Zip Code:
Contact:	Phone No.:	Fax No.:	E-mail:
Subcontract Amount:	Percentage:	Description of Work:	
Is your company a certified HUB? <input type="checkbox"/> Yes <input type="checkbox"/> No	Indicate Gender & Ethnicity:		
Certifying Agency (Check all applicable):	<input type="checkbox"/> State of Texas (HUB)	<input type="checkbox"/> City of Austin (M/WBE)	<input type="checkbox"/> Texas Unified Certification Program (TUCP) (DBE)

**SECTION 4 DISCLOSURE OF NON-HUB SUBCONTRACTORS**

(Duplicate as necessary)

Travis County exercises the right to verify subcontractors listed on this project.

Sub Company Name:		State of Texas VID#:	
Address:	City:	State:	Zip Code:
Contact:	Phone No.:	Fax No.:	E-mail:
Subcontract Amount:	Percentage:	Description of Work:	

Sub Company Name:		State of Texas VID#:	
Address:	City:	State:	Zip Code:
Contact:	Phone No.:	Fax No.:	E-mail:
Subcontract Amount:	Percentage:	Description of Work:	

Sub Company Name:		State of Texas VID#:	
Address:	City:	State:	Zip Code:
Contact:	Phone No.:	Fax No.:	E-mail:
Subcontract Amount:	Percentage:	Description of Work:	

Sub Company Name:		State of Texas VID#:	
Address:	City:	State:	Zip Code:
Contact:	Phone No.:	Fax No.:	E-mail:
Subcontract Amount:	Percentage:	Description of Work:	

**SECTION 5 NON-COMPLIANT FOR MEETING SET HUB GOALS CHECKLIST**

If you were unable to meet the set goals for this project, select the box by the response(s) that best fits your situation.

- ☐ All subs to be utilized are "Non-HUBs."
 ☐ HUBs solicited did not respond.
- ☒ HUBs solicited were not competitive.
 ☐ HUBs were unavailable for the following trade(s):

**SECTION 6 DETERMINATION OF "GOOD FAITH EFFORT" (GFE) CHECKLIST**

The following checklist shall be completed by the Bidder and returned with the response. This list contains the minimum efforts that should be put forth by the Bidder when attempting to achieve or exceed the HUB goals. The Bidder may go beyond the efforts listed below. If additional information is needed, the Bidder will be contacted by the HUB Program Staff. Select the box that describes your efforts.

- ☒ Divide the contract work into the smallest feasible portions to allow for maximum HUB Subcontractor participation, consistent with standard and prudent industry practices.
- ☒ Notify HUBs of work that the prime contractor plans to subcontract, allowing sufficient time for effective participation?  
The HUB Program encourages that three or more HUBs be notified per scope of work and given no less than five working days to respond. (The notification should contain adequate information about the project i.e. plans, specifications, and scope of work; Bonding and insurance requirements of the HUB subcontractor; and a point of contact within the Bidders organization.)
- ☐ If a bid was requested from a HUB and then rejected, was a written rejection notice detailing the reasons why they were not selected issued?  
If yes, provide a copy of the rejection letter.
- ☐ Provide notices of opportunities to minority or women trade organizations or development centers to assist in identifying potential HUBs by disseminating the information to their members/participants? If yes, attach correspondence.
- ☐ Bidder has (0) zero HUB participation. Provide an explanation



**SECTION 7 RESOURCES**

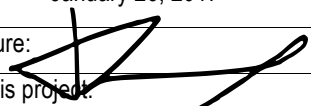
TRADE ASSOCIATIONS	PHONE (512)	FAX	E-mail/website
Asian Construction Trade	926-5400	926-5410	<a href="http://www.acta-austin.com">www.acta-austin.com</a>
Austin Black Contractors	467-6894	467-9808	<a href="http://www.abcatx.com">www.abcatx.com</a>
Austin Metropolitan United Black Contractors	784-1891	255-1451	<a href="mailto:unism@sbcglobal.net">unism@sbcglobal.net</a>
<b>Natl. Assoc. of Women in Construction</b>	476-5534	476-8337	
<b>US Hispanic Cont. Assoc. de Austin</b>	922-0507	374-1421	<a href="http://www.ushca-austin.com">www.ushca-austin.com</a>
CERTIFYING AGENCIES TRAVIS COUNTY RECOGNIZES		CERTIFYING AGENCIES VENDOR DATABASE WEBSITES	
State of Texas Centralized Master Bidders List	<a href="http://www.cpa.state.tx.us/business.html">www.cpa.state.tx.us/business.html</a>		CMBL includes certified HUBs.
City of Austin Minority Vendor Database	<a href="http://www.austintexas.gov/department/small-and-minority-business">www.austintexas.gov/department/small-and-minority-business</a>		Certified Vendors Directory
Texas Unified Certification Program	<a href="http://www.dot.state.tx.us/business">www.dot.state.tx.us/business</a>		TUCP DBE Directory

**SECTION 8 AFFIRMATION**

As evidenced by my signature below, I certify that all the information provided is correct to the best of my knowledge. I am an authorized representative of the Bidder listed in SECTION 1, and that the information and supporting documentation submitted with HUB Forms are correct and true to the best of my knowledge.

Bidder understands and agrees that, if awarded any portion of the solicitation:

- The Bidder must either utilize Travis County HUB Programs Vendor Tracking System (VTS) to report payments to sub-contractors on a monthly basis or submit monthly Payment Reports as requested by the HUB Program Coordinator.
- The Bidder must seek pre-approval from the HUB Program Coordinator prior to making any modifications to their HUB Sub-contracting Plan. The Bidder must complete a HUB Subcontractor/Subconsultant Change Form obtained from the HUB Program Staff. Return form via fax to 512-854-9185 or email [hubstaff@co.travis.tx.us](mailto:hubstaff@co.travis.tx.us).
- Travis County HUB Program Staff will perform a Good Faith Effort (GFE) Review, documenting the efforts put forth by the Bidder.

Name and Title:	Jodee LeRoux	Date:	January 26, 2017
E-mail Address:	<a href="mailto:contracts@galois.com">contracts@galois.com</a>	Signature:	
Provide contact information for the individual in your office who will handle invoicing for this project.			
Name and Title:	Peni Northcott	E-mail Address:	<a href="mailto:invoice@galois.com">invoice@galois.com</a>
Phone No.:	503-808-7200	Fax No.:	503-350-0833

Please be reminded that Travis County is not party to your agreement executed with the subcontractors and subconsultants.

## **Qualifications Questionnaire/Firm Experience and Qualifications**

## **QUALIFICATIONS QUESTIONNAIRE**

This questionnaire is to be completed in its entirety. No modifications to the wording is permitted. Proposals submitted with Qualifications Questionnaires that are incomplete or incorrect, or that have been altered, are subject to rejection.

**1. Name of Firm:**

Galois, Inc., dba Free & Fair

**2. Address of Headquarters:**

421 SW 6th Avenue, Suite 300  
Portland, Oregon 97204

**3. Address of Local Office If Different:**

N/A

**4. Date of Organization (Month/Year):**

October 1999

**5. Names and Dates of Predecessor Organization(s):**

None

**6. Type of Organization:**

Corporation

**7. Business Telephone and Fax Number(s):**

Telephone 971.808.3247, Fax 503.350.0833

**8. List of Principals, Titles, Degrees:**

- Joseph Kiniry, Free & Fair CEO/Chief Scientist, Ph.D. in Computer Science from Caltech
- Rob Wiltbank, Galois CEO, Ph.D. in Strategic Management from the University of Washington
- Daniel Boyer, Galois CFO, MBA & JD from Willamette University

## QUALIFICATIONS QUESTIONNAIRE (cont.)

### FIRM EXPERIENCE AND QUALIFICATIONS

**9. Years of Experience** - Number of years performing proposed services:  
17 years of performing high assurance systems engineering; 15 years of elections-related R&D.  
Details of expertise of principals involved is included in the “Project Staff” section below.

**10. Firm experience** - Briefly describe three or more projects of similar content for each of the Elements contained in your proposal and include approximate duration and dollar value of the projects.

Element B, Table 1: Projects illustrating firm's relevant experience for

Duration of Project	Project Description	Dollar Value
4 years	<b>High Assurance Cyber Military Systems (HACMS).</b> Funded by the Department of Defense, we developed tools that help create “hack-proof” software for land, air, and sea vehicles, as part of DARPA’s HACMS program. The tools can be used to automatically generate safe low-level vehicle software instead of writing it by hand, in order to rule out a vast array of vulnerabilities. We will use similar technologies to generate parts of the STAR-Vote system. The HACMS tools are deployed at Boeing, where they are used on the Unmanned Little Bird, an autonomous combat helicopter, to ensure that the vehicle’s communications software is safe and secure. We continue to develop and maintain these Open Source tools.	\$4M
3 years	<b>Copilot.</b> Funded by NASA, we built Copilot to detect avionics hardware failures before they become catastrophic. Copilot creates distributed software monitors designed to detect pitot tube failures, which have been implicated in numerous commercial aircraft incidents and accidents. The software was tested and proven to be successful in helping detect failures before they cause accident. Copilot is an open source project hosted by us and is currently deployed at NASA.	\$600K
17 years	<b>Cryptol.</b> Funded by the NSA’s Trusted Systems Research Group, Cryptol is an advanced tool suite for creating and verifying encryption software specifications. For more than a decade, we have actively developed, maintained, and supported Cryptol as it has been deployed across defense and intelligence agencies. As of 2013, Cryptol is also publicly available and Open Source, with continued	>\$10M

### QUALIFICATIONS QUESTIONNAIRE (cont.)

Duration of Project	Project Description	Dollar Value
	development taking the same approach as STAR-Vote development proposed here. Cryptol is a prime example of our proven success in deploying and maintaining highly advanced technology.	
6 years	<b>Software Analysis Workbench (SAW).</b> SAW is a set of tools designed to help scientists and engineers formally verify computer programs, establishing mathematical guarantees that they do not contain flaws and vulnerabilities. Developed and maintained by us, SAW has been deployed in conjunction with Cryptol to verify the correctness of multiple cryptographic algorithms. SAW is also Open Source, and we continue to maintain and develop it.	\$4.1M
3 years	<b>CyberChaff.</b> CyberChaff is a network defense tool that uses cyber deception to detect hackers and trick them into revealing themselves. Originally developed through a contract with the Department of Defense, CyberChaff takes an innovative approach to reduce the likelihood that an advanced attacker will find valuable resources in an organization. We have most recently deployed CyberChaff at Reed College. CyberChaff is also deployed at a Fortune 50 company and has been licensed to third parties for further deployment in private organizations and integration in their own products. The software is another good example of our capability to deploy and support advanced technology.	\$1.2M
1 year	<p><b>Amazon s2n.</b> Amazon's s2n is a Transport Layer Security (TLS) library. Amazon is taking steps to make it the most reliable and secure library available; as part of that effort Amazon asked us to verify a number of cryptographic algorithms included in the code. We were able to perform the verification, reducing hundreds of lines of code to a much smaller and easier to understand specification.</p> <p>Amazon management has strict reporting requirements to ensure that their projects are on track and providing value to the company. To comply with their tracking requirements, we integrated our verification project into their continuous integration system. Any time any changes are made to the</p>	\$800K

### QUALIFICATIONS QUESTIONNAIRE (cont.)

Duration of Project	Project Description	Dollar Value
	<p>s2n code, our tools are run to make sure the changes are correct.</p> <p>We took this integration a step further in order to report the progress of our test runs to Amazon. Our tests automatically output their results. We provided Amazon with software that automatically processes the continuous integration logs to display easily-digested statistics about the success of test runs and the progress that has been made.</p>	

Element C, Table 1: Projects illustrating firm's relevant experience

Duration of Project	Project Description	Dollar Value
8 months	<p><b>SHAVE.</b> The goal of SHAVE is to inform about, and assess the feasibility of, a practical end-to-end assurance case for mission critical systems that run on COTS and bespoke hardware. The SHAVE demonstrator is an inline streaming encryption engine realized on RISC-V, a modern open source processor. Such a device is comparable to the “bump-in-wire” encryption devices deployed today within the Department of Defense, except that it will include a formal assurance case to show that it is perfectly fit for purpose, correct, and secure. It will be realized via a cryptographic extension to RISC-V, a small formally verified firmware layer for interacting with that extension, and a lightweight API atop the firmware layer to make it accessible to programming languages like C and Rust. Within SHAVE we also are producing the SHAVE formal method for building the aforementioned end-to-end assurance case.</p>	\$500K
18 months	<p><b>GULPHAAC.</b> Free &amp; Fair principals invented the Galois Ultra Low Power High Assurance Asynchronous Cryptography (GULPHAAC) chip which represents an entirely new technology for the automatic generation of hardware designs for chip (ASIC) fabrication. The demonstration system that we built is the world’s first formally verified cryptography chip, and is also the world’s first asynchronous (clockless) crypto chip. The chip operates at threshold voltage; it is therefore extremely low power and low energy, and is energy-competitive with the</p>	\$700K



### **QUALIFICATIONS QUESTIONNAIRE (cont.)**

<b>Duration of Project</b>	<b>Project Description</b>	<b>Dollar Value</b>
	lowest energy devices ever invented. The chip is power invariant—if provided more voltage it runs faster—and is consequently speed competitive with the best chips on the market. Finally, the chip has an assurance case far in excess of any crypto chip on the market.	
4 months	<b>Undisclosed Client.</b> Free & Fair principals were responsible for performing a hardware and software quality and security audit of an authentication system designed to be used by members of the intelligence community in the field.	\$90K

**11. Project References** - Describe at least three projects for each Element your proposal includes on which the firm has provided similar products or services within the last five years. Include a description of the products or services, location of project, and the name, address, and telephone number of at least one person representing the client who received the products or services. If proposing more than one Element, add additional tables as required.

**Element B, Table 4: Project Reference #1**

<b>Location:</b> Washington, DC		<b>Date(s) of Work:</b> Mar 2015 – Sep 2016
<b>Description of Goods and Services:</b> <i>Private Elections Quality and Security Audits.</i> Within this project, Free & Fair principals performed a quality and security audit of an Internet Voting system used by most unions in the USA, and also provided expert input into national policy in union elections.		
<b>Reference Contact Information:</b>		
Company Name:	US Department of Labor	
Contact Full Name:	Leonard Tambra	
Contact Mailing Address:	200 Constitution Avenue NW, Suite N-2474 Washington DC 20210	
Contact Email Address:	leonard.tambra@dol.gov	
Contact Telephone Number	(202) 693-5744	

## QUALIFICATIONS QUESTIONNAIRE (cont.)

Element B, Table 4: Project Reference #2

<b>Location:</b> Portland, OR	<b>Date(s) of Work:</b> Nov 2015 – Mar 2016
<b>Description of Goods and Services:</b> <i>C11 Verification Technology.</i> Within this project, Free & Fair principals created formal verification technology for the National Institute of Standards and Technology (NIST). This technology focuses on verifying properties of modern C code, which uses new keywords to enable developers to specify the use of novel memory models for modern multi-core systems.	
<b>Reference Contact Information:</b>	
Company Name:	National Institute of Standards and Technology (NIST)
Contact Full Name:	Paul Black
Contact Mailing Address:	100 Bureau Drive, Stop 8970 Gaithersburg, MD 20899-8970
Contact Email Address:	paul.black@nist.gov
Contact Telephone Number	(301) 975-4794

Element B, Table 4: Project Reference #3

<b>Location:</b> Portland, OR	<b>Date(s) of Work:</b> Mar 2015 – Oct 2016
<b>Description of Goods and Services:</b> <i>Galois Ultra Low Power High Assurance Asynchronous Cryptography.</i> Within this project, Free & Fair principals invented the Galois Ultra Low Power High Assurance Asynchronous Cryptography (GULPHAAC) chip, which represents an entirely new technology for the automatic generation of hardware designs for chip (ASIC) fabrication. The demonstration system that we built is the world's first formally verified cryptography chip, and is also the world's first asynchronous (clockless) crypto chip. The chip operates at threshold voltage; it is therefore extremely low power and low energy, and is energy-competitive with the lowest energy devices ever invented. The chip is power invariant—if provided more voltage it runs faster—and is consequently speed competitive with the best chips on the market. Finally, the chip has an assurance case far in excess of any crypto chip on the market.	
<b>Reference Contact Information:</b>	
Contact Full Name:	Bryan Weeks

**QUALIFICATIONS QUESTIONNAIRE (cont.)**

Contact Mailing Address:	9800 Savage Road, Suite 6845 Fort Meade MD 20755-6845
Contact Email Address:	beweeks@tycho.ncsc.mil
Contact Telephone Number	(443) 634-3936

**Element C, Table 4: Project Reference #1**

<b>Location:</b> Portland, OR	<b>Date(s) of Work:</b> Mar 2015 – Oct 2016
<b>Description of Goods and Services:</b>  <i><b>Galois Ultra Low Power High Assurance Asynchronous Cryptography.</b></i> Within this project, Free & Fair principals invented the Galois Ultra Low Power High Assurance Asynchronous Cryptography (GULPHAAC) chip, which represents an entirely new technology for the automatic generation of hardware designs for chip (ASIC) fabrication. The demonstration system that we built is the world's first formally verified cryptography chip, and is also the world's first asynchronous (clockless) crypto chip. The chip operates at threshold voltage; it is therefore extremely low power and low energy, and is energy-competitive with the lowest energy devices ever invented. The chip is power invariant—if provided more voltage it runs faster—and is consequently speed competitive with the best chips on the market. Finally, the chip has an assurance case far in excess of any crypto chip on the market.	
<b>• Reference Contact Information:</b>	
Contact Full Name:	Bryan Weeks
Contact Mailing Address:	9800 Savage Road, Suite 6845 Fort Meade MD 20755-6845
Contact Email Address:	beweeks@tycho.ncsc.mil
Contact Telephone Number	(443) 634-3936

**Element C, Table 4: Project Reference #2**

<b>Location:</b> Portland, OR	<b>Date(s) of Work:</b> Nov 2015 – Mar 2016
<b>Description of Goods and Services:</b>  <i><b>C11 Verification Technology.</b></i> Within this project, Free & Fair principals created formal verification technology for the National Institute of Standards and Technology (NIST). This technology focuses on verifying properties of modern C code, which uses new keywords to enable developers to specify the use of novel memory models for modern multi-core systems.	

### QUALIFICATIONS QUESTIONNAIRE (cont.)

<b>Reference Contact Information:</b>	
Company Name:	National Institute of Standards and Technology (NIST)
Contact Full Name:	Paul Black
Contact Mailing Address:	100 Bureau Drive, Stop 8970 Gaithersburg, MD 20899-8970
Contact Email Address:	paul.black@nist.gov
Contact Telephone Number	(301) 975-4794

Element C, Table 4: Project Reference #3

<b>Location:</b> Portland, OR	<b>Date(s) of Work:</b> Jun 2014 – Jul 2015
<b>Description of Goods and Services:</b> <i><b>Future of Voting.</b></i> Within this project, Free & Fair principals led a research study into the feasibility of End-to-End Verifiable Internet Voting (E2E-VIV), and edited and co-authored a 136-page report with several technical appendices that lays out the necessary and sufficient conditions for the realization of such an ambitious but controversial system. This project also necessitated the management of an extremely diverse team of international experts in relevant topics—a team that was at odds internally given the nature of the topic and heated opinions about security, enfranchisement, policy, and more. Some of the technical elements of this project, particularly its informal domain model of elections and core ideas about cryptographic framing of E2E-V systems, are directly relevant to the STAR-Vote project. This report is now the de facto reference for all R&D in internet voting.	
<b>Reference Contact Information:</b>	
Contact Full Name:	Susan Dzieduszycka-Suinat
Contact Mailing Address:	U.S. Vote Foundation 4325 Old Glebe Road Arlington, VA 22207 USA
Contact Email Address:	susan@usvotefoundation.org
Contact Telephone Number	+49 (0) 89 64939133

## QUALIFICATIONS QUESTIONNAIRE (cont.)

Element C, Table 4: Project Reference #4

<b>Location:</b> Portland, OR		<b>Date(s) of Work:</b> Sept 2014 – present
<b>Description of Goods and Services:</b> <i>SHAVE</i> . The goal of SHAVE is to inform about, and assess the feasibility of, a practical end-to-end assurance case for mission critical systems that run on COTS and bespoke hardware. The SHAVE demonstrator is an inline streaming encryption engine realized on RISC-V, a modern open source processor. Such a device is comparable to the “bump-in-wire” encryption devices deployed today within the Department of Defense, except that it will include a formal assurance case to show that it is perfectly fit for purpose, correct, and secure. It will be realized via a cryptographic extension to RISC-V, a small formally verified firmware layer for interacting with that extension, and a lightweight API atop the firmware layer to make it accessible to programming languages like C and Rust. Within SHAVE we also are producing the SHAVE formal method for building the aforementioned end-to-end assurance case.		
<b>Reference Contact Information:</b>		
Contact Full Name:	Linton Salmon (Program Manager) and Marnie Dunsmore (SETA)	
Contact Mailing Address:	DARPA 675 N Randolph St Arlington, VA 22203	
Contact Email Address:	linton.salmon@darpa.mil marnie.dunsmore.ctr@darpa.mil	
Contact Telephone Number	(703) 526-2886 ext. 2886	

12. Attach a Management Chart showing the Project team members, areas of responsibility, and team organization structure.

## **QUALIFICATIONS QUESTIONNAIRE (cont.)**

**13. Project Staff** – List the name of the person who will be directly responsible for performance of the Project services and indicate the number of years of experience managing projects of similar size. Attach resume(s) describing specific related experience.

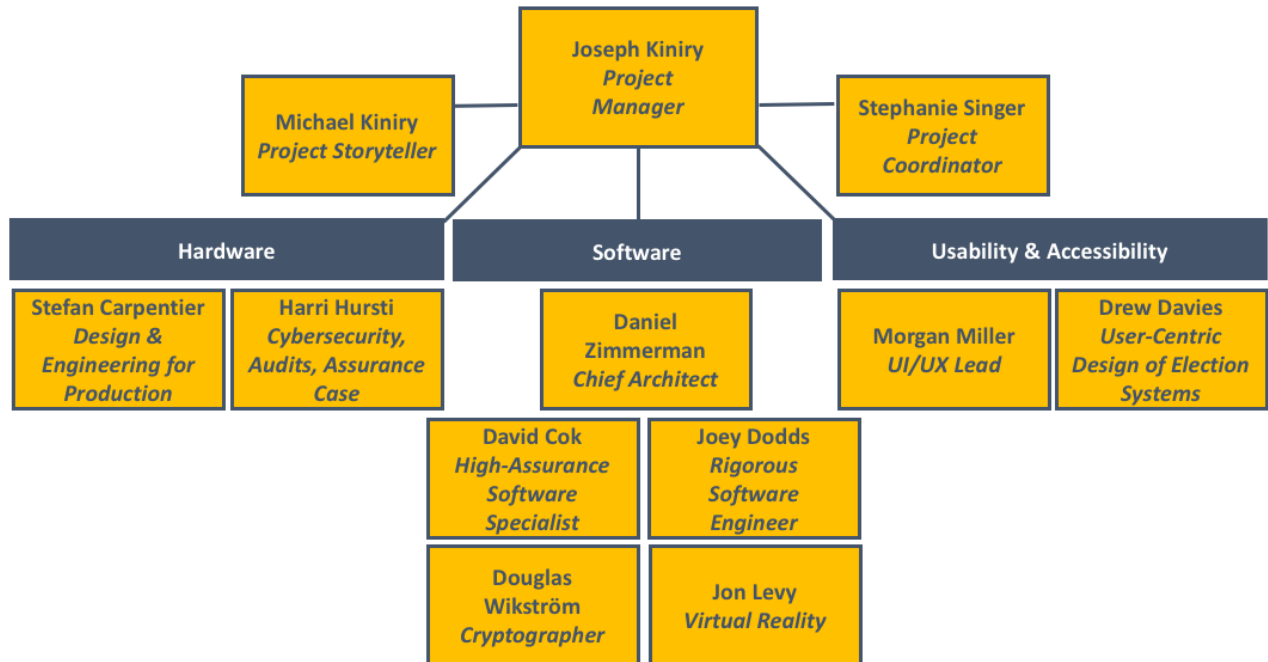
**Table 5: List of Project Staff**

<b>Name</b>	<b>Position/Title</b>	<b>Years of Experience</b>
Dr. Joseph Kiniry	Project Manager	22
Dr. Daniel Zimmerman	Chief Architect	15
Dr. Joey Dodds	Rigorous Systems Engineer	9
Dr. Stephanie Singer	Project Coordinator	12
Dr. David Cok	High-Assurance Software Specialist	32
Dr. Douglas Wikström	Cryptographer	16
Jon Levy	Virtual Reality Design Director	27
Michael Kiniry	Project Storyteller	13
Morgan Miller	UI/UX Lead	7
Drew Davies	User-Centric Design of Election Systems UI Expert	22



## QUALIFICATIONS QUESTIONNAIRE (cont.)

### 1 Attachment: Project Management Chart



## **QUALIFICATIONS QUESTIONNAIRE (cont.)**

### 2 Attachment: Project Staff Resumes

#### 2.1 Dr. Joseph Kiniry, Project Manager

Dr. Joseph Kiniry, Ph.D., is Chief Scientist and CEO of Free & Fair. Prior to working for Free & Fair, Dr. Kiniry provided commercial and public consultancy services to several governments on matters relating to elections, their technology, security, processes, and verifiability. He has worked on election systems for thirteen years; has audited the security, correctness, and reliability of numerous physical and Internet-based voting systems; has developed high-assurance prototypes and products of several election technologies (including, but not limited to, tallying, auditing, voting, ballot marking, and e-poll book (EPB) systems); and sits on the Board of Advisors of the main verifiable elections nonprofit, Verified Voting.

Dr. Kiniry has formally advised four governments (the USA, The Netherlands, the Republic of Ireland, and Denmark) on matters relating to digital elections and has testified before two parliaments. He has also provided informal input and advice to the governments of Norway, Estonia, and the United States. He co-founded and co-ran a multi-year research project on digital elections (the DemTech project<sup>1</sup>) and has supervised numerous BSc, MSc, and PhD theses focusing on elections technologies. His research group has developed several high-assurance peer-reviewed election software systems, including a tally system used in binding European elections for The Netherlands and an EPB system for in Danish national elections. Dr. Kiniry has served as a Principal Investigator on teams for the European Union Council, various DoD branches, the National Science Foundation, and several national funding agencies in Ireland, The Netherlands, and Denmark.

Dr. Kiniry also regularly interacts with and provides input to federal agencies related to elections including the EAC, NIST, and FVAP, and several elections-related non-profits including the OSET Foundation, Common Cause, Democracy Works, the Overseas Vote Foundation, and U.S. Vote. He is a key actor in the newly formed NIST-EAC Public Working Groups.

#### 2.2 Dr. Daniel Zimmerman, Chief Architect

Dr. Daniel Zimmerman, Ph.D., Chief Architect at Free & Fair, has extensive experience in formal methods, high-assurance software engineering, concurrent and distributed systems, and foundations of computer science. He taught computer science at multiple universities for over a decade. In industry, Dr. Zimmerman has worked primarily in the areas of rigorous software engineering and verifiable elections technology. He is a member of the Elections Verification Network.

---

<sup>1</sup> <http://demtech.dk/>

## **QUALIFICATIONS QUESTIONNAIRE (cont.)**

### **2.3 Dr. Joey Dodds, Rigorous Software Engineer**

Dr. Joey Dodds, Ph.D., will be a key performer in the implementation and verification of STAR-Vote. He recently received his Ph.D. from Princeton University, where he researched proving correctness of C programs including cryptographic algorithms. At Free & Fair, Dr. Dodds has implemented both a tabulator and a risk limiting audit system and done specifications for both. He also fully proved the correctness of the tabulator. He is a key participant in the verification of Amazon's s2n library. He has been responsible for both the verification of the library and implementing a system to automatically report metrics about the progress of the project to Amazon's upper management.

### **2.4 Dr. Stephanie Singer, Project Coordinator**

Dr. Stephanie Singer, Ph.D., has dual expertise in technology and elections. She studied computer science at Stanford University, earned a Ph.D. in Mathematics from New York University, held a tenured professorship at Haverford College, and worked in the private sector as a data strategist and technology manager. She has extensive experience with elections over more than a decade in roles ranging from poll worker to candidate to election data analyst to Chair of the Philadelphia County (Pennsylvania) Board of Elections. She served four years as elected City Commissioner in Philadelphia. For three years, she served on the Board of the County Commissioners Association of Pennsylvania and as Co-Chair of the statewide Elections Reform Committee of that organization.

### **2.5 Dr. David Cok, High-Assurance Software Specialist**

Dr. David Cok, Ph.D., will contribute to the project as an expert in software verification systems and in transitioning research ideas into practical software tools. At Eastman Kodak, he was a senior researcher with many patents to his credit, led scientific research labs, and led development groups that implemented novel image processing algorithms in commercial products. Over the past 20 years, he has also developed systems for formal verification of software, both as open source tools and in support of U.S. government research contracts. In particular, he brings expertise in the translation of current programming languages (such as Java, C, LLVM) to logical representations and in applying logical tools, such as automated SMT solvers, that can verify assertions about practical programs. Dr. Cok has served as Principal Investigator on teams for NASA, various DoD branches, and the National Science Foundation.

## **QUALIFICATIONS QUESTIONNAIRE (cont.)**

### 2.6 Dr. Douglas Wikström, Cryptographer

Dr. Douglas Wikström, Ph.D., is an associate professor in cryptography at KTH Royal Institute of Technology. He researches theoretical cryptography, but ever since 2000 he has spent part of his time on cryptographic aspects of electronic voting systems and his thesis focused on mix-nets. Today he is considered to be a world-leading expert on this topic.

He founded the company Verificatum AB in 2011 to refine the mix-net implementation he completed 2008 into an industrial grade product. He invented key mix-net components that have since been adopted in the Helios and the UniVote voting systems, but he has also discovered several practical attacks and vulnerabilities of mix-nets proposed in the literature, e.g., Civitas, a version of Scantegrity, and the scheme provided by Scytl to Norway 2011.

He has co-chaired the EVOTE conference and served on several program committees of conferences in the field, and he has served as an expert at hearings of Swedish government committees as well as the Swedish Voting Authority multiple times. He is a member of the Election Verification Network (EVN).

### 2.7 Jon Levy, Design Director (AMA Studios)

Jon Levy is an Emmy Award-Winning Design Director with two decades of experience delivering projects for Fortune 100 firms including Activision, Sony, Nike, MIT, US Army, ABC, Warner Bros, and Disney. He has organized creative teams across international locations, including the Philippines, India and Brazil. His extensive portfolio includes Industrial Design, Environmental Design, Visualization, and Interactive development. In addition to being the Director of AMA Studios, Jon is the Manager of the NASA Advanced Concepts Laboratory (ACL). The ACL is a digital creation studio located on the Langley Research Center. The ACL in the unique position of participating in a wide array of early stage NASA projects. The ACL gives form to technologies, projects and programs by clarifying the design and communicating the story.

### 2.8 Michael Kiniry, Project Storyteller

Michael Kiniry, Communicator at Free & Fair, is a media expert with backgrounds in radio, print, and photojournalism. He spent nearly a decade as a public radio reporter, producer, and host and has been a freelance photographer and writer for the past 14 years. Mike is also a videographer and editor and is the EVN's dedicated videographer/producer.

### 2.9 Morgan Miller, UI/UX Lead

Morgan Miller is an experienced User Experience (UX) professional with a deep background in scientific research. She is currently a User Experience Architect for Morgan Miller UX, LLC, where she leads teams through a UX discovery, architecture, and research process; designs and executes research studies; synthesizes research data to create actionable recommendations; and builds information architecture including taxonomy, sitemaps, and wireframes. She has done work for Overseas Vote Foundation, Intel, Mozilla Foundation, BMC Software, Esri, World Wildlife Fund, Nike, Moda, Providence Health, and Cambia Health. She earned a B.A. in Mathematics from Reed College and an M.S. in Computer Science from the University of Lugano, Switzerland, where she was a cryptography researcher.

## **QUALIFICATIONS QUESTIONNAIRE (cont.)**

### 2.10 Drew Davies, User-Centric Design of Election Systems UI Expert (Oxide Design Co.)

Oxide Design Co. is a branding and design firm established in 2001. During the past 15 years, Oxide's work has been awarded by every major design competition, including One Show Design, the CLIO Awards, and six different times by *Communication Arts Design Annual*. Oxide's clients range from one-person startups to Fortune 200 companies, across a multitude of industries. Their work spans the consumer/retail, business-to-business, and public/civic design spaces.

Because Oxide believes very strongly in the power of design to create progressive change, over 50 percent of Oxide's work is donated — in whole or in part — to a wide range of non-profit and charitable organizations.

Oxide is heavily active in the national civic design space, working regularly with states, counties, and federal government agencies, including New York State Board of Elections, California Secretary of State, Virginia Board of Elections, and Pennsylvania Department of State. Oxide worked with the Federal Voting Assistance Program (FVAP) to redesign both the online and print versions of the Federal Post Card Application (FPCA) and Federal Write-in Absentee Ballot (FWAB), as well as the Voting Assistance Guide, for overseas voters. In addition, Oxide served as part of the core design and research team that developed the U.S. Election Assistance Commission's national ballot design standards, and subsequently helped develop the Field Guides to Ensuring Voter Intent — pocket-sized guides containing field-researched, critical election design techniques that help ensure that every vote is cast as voters intend.

One of Oxide's most notable contributions in civic design is developing the Anywhere Ballot — an online ballot marking interface — in partnership with the Center for Civic Design and the University of Baltimore. The project created a thoroughly tested, highly usable tool allowing U.S. military and overseas citizens — as well as persons with physical or cognitive disabilities — to vote more easily. Anywhere Ballot's ultimate goal is to allow every citizen to vote on any device, anywhere, at any time.

### 2.11 Harri Hursti (Nordic Innovation Labs)

Harri Hursti is one of the world's foremost experts on the topic of electronic voting security, having served in all aspects of the industry sector. He is an authority on uncovering critical problems in electronic voting systems worldwide, including in the U.S., Finland, Estonia, the Philippines, and Argentina. As a consultant, he has conducted and co-authored many studies, both academic and commercial, on numerous election systems' data security and vulnerabilities. These studies have come at the request of officials, legislators and policy makers in 5 countries; including the U.S. government, at both the state and federal level. Mr. Hursti is famously known for his successful attempt to demonstrate how the Diebold Election Systems' voting machines could be hacked, ultimately altering final voting results. Hursti performed two voting machine hacking tests which became widely known as the *Hursti Hacks*. The Hursti Hack tests were filmed and turned into an acclaimed HBO documentary called *Hacking Democracy* which was nominated for an Emmy award for outstanding investigative journalism. Mr. Hursti received the EFFI Winston Smith Award in 2008 and the EFF Pioneer Award in 2009 for his work in election security.

## **QUALIFICATIONS QUESTIONNAIRE (cont.)**

### 2.12 Maggie MacAlpine (Nordic Innovation Labs)

Margaret “Maggie” MacAlpine is an election auditing specialist and system testing technologist who has worked on a variety of projects that include electronic testing of voting registration systems, election security and election fraud. Highly specialized technologist in testing and performing risk limiting and transitive audits on election results, she has consulted on multiple projects in Florida, Connecticut, and Colorado. She has served as an advisor for the office of the Secretary of State of California for the Risk Limiting Audit Pilot Program 2011-2012, and is widely regarded as an expert on the use of high-speed scanners for conducting post-election audits. Ms. MacAlpine was a contributing researcher on the “Security Analysis of the Estonian Internet Voting System” in partnership with the University of Michigan.

### 2.13 Stefan Carpentier (Design SHIFT)

Stefan Carpentier delivered successful engineering management in a variety of fields including Consumer Electronic Design, Semiconductor Design, Software Design and MEMs Design. Development in close cooperation with the customer, on time, on/under budget, on target. Working with people and building fair, innovative, beautiful products is what makes him “tick”.

### 2.14 Daniel Nelson (Design SHIFT)

Daniel Nelson specializes in software test methodology and navigating the complexities of legal conformance, platform supplier approval, and wireless network operator approval. He has deep expertise in multiple categories of consumer electronics including tablets, smartphones, GPS Navigation devices, and handheld/pocket organizers on multiple software platforms including Microsoft Windows CE (and Windows Mobile), Symbian (UIQ and Series 60), Linux, and Google Android. Daniel is currently engaged in the validation and compliance activities surrounding Android-based tablets and other CE products. He was previously the Validation Manager for TomTom Inc, covering all testing (hardware and regional software variance), compliance, and approvals activities in North and South America. Positions prior to TomTom include Validation Manager for Symbian Smartphone Development at Motorola, and Test and Automation Lead at Sendo.

## **Insurance Requirements**

Free & Fair is currently insured for the following required coverages:

- Workers' Compensation and Employers' Liability
- Commercial General Liability
- Business Automobile Liability
- Professional Liability/E&O
- Umbrella Liability
- Cyber Security

Should an award be made, we will be able to have the necessary insurance documentation provided to Travis County within ten (10) calendar days after award and before beginning work.