FREE & FAIR

Response to Request for Information
Voting System Assessment Project (VSAP)
RFI #17-001

Free & Fair
421 SW 6th Ave., Suite 300
Portland, OR 97204

26 March 2017

Table of Contents

1.0 Respondent Identifying Information

Vendor Profile	
Company Name	Galois d/b/a Free & Fair
Name of Parent Company	
Type of Legal Entity (e.g., Corporation, Partnership, Limited Liability Company, etc.)	Class C Corporation
Company Headquarters City/State	Portland, OR
Authorized Contact (First and Last Name)	Dr. Joseph Kiniry
Title	CEO and Chief Scientist
Office Address	421 SW 6th Ave, Suite 300 Portland, OR 97204
Phone Number	503-626-6616
Email Address	contact@freeandfair.us
Number of Full Time Employees	62
Last Fiscal Year Company Revenue	$24M
% of Revenue from State and Local Government Clients in the United States	0%
% of Revenue from IT Design and Implementation Services	>90%

Number of Years Vendor has been Providing the Type of Services Specified in this RFI – Describe briefly	Number of years performing proposed services: 17 years of performing high assurance systems engineering; 15 years of election-related R&D. Details of expertise of principals involved is included in the "Project Staff" section below.
Number of Projects Vendor has Delivered Related to the Type of Services Specified in this RFI **– Describe briefly**	In excess of 100 projects over the past 17 years; see the previous answer for more information. Galois was founded 17 years ago as a spin-out from the Oregon Graduate Institute. Galois has delivered complex secure software systems to federal government clients at the Department of Defence, Intelligence Community, Homeland Security, NIST, and other agencies for 17 years. Many of these projects were multi-year efforts that included complex, edge-of-discipline R&D and entailed working with multiple subcontractors and clients.

3.0 Vendor Background and References

3.1 Vendor Background

Free & Fair's mission is to bring open source, high-assurance, end-to-end verifiable elections to the world. In this response, Free & Fair[1] proposes to create an open source, high assurance solution for all of Los Angeles County's components. This system will fulfill the technical requirements stipulated in the RFI, and will leverage as much existing technology (commercial or open source) as possible.

Free & Fair is exactly the right entity to realize Los Angeles County's vision because we have:

- world-class expertise in high assurance open source election systems and risk-limiting audits,
- an unparalleled record 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 focus on transparency, security, and affordability.

We further describe our company and reflect upon these points in the following pages.

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

World-class Expertise

Our world-class expertise is concretized in three main dimensions relevant to Los Angeles County:

- 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 commercial off-the-shelf (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 contributions 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 election integrity and scientific communities 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 excellent subcontractors. We commonly work with world-class firms, small and large, as well as top universities in achieving our ambitious research, development, and engineering goals.

On Time and On Budget

Free & Fair's principals and this project team have ample experience delivering provably secure technology to government, on time and on budget. We can provide a large set of projects that were delivered on time and on budget.

Free & Fair is already deeply familiar with election technology. We expect to develop systems quickly based on our experience developing Free & Fair's existing products and demonstrator components, which already implement much of the desired VSAP functionality. Over the past year we have developed prototype election 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 election technology and to demonstrate the style and quality of our software development capabilities. 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 VSAP system.

Open Source Veterans

Traditionally, election technology vendors have profited from limited competition and ownership of proprietary systems. Free & Fair has a different business model. We understand the budget constraints that jurisdictions face, and welcome 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 develop 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 Commercial off-the-shelf (COTS).

Security for "Critical Infrastructure"

In January 2017, in response to the increasing sophistication of adversaries who might wish to attack or disrupt U.S. elections, the DHS officially designated U.S. election systems "critical infrastructure" on par with systems vital to energy, financial services, healthcare, transportation, agriculture, and communications.

Free & Fair has 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.

We will build election technology that meets the highest standards for software design and security, such as those stipulated by the U.S. National Institute of Standards and Technology (NIST) and similar agencies in Canada. 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 totalling over $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 has the capacity not merely to build VSAP components, but to make them as secure as the other systems already designated "critical infrastructure" by DHS.

NIST Special Publication 800-160[2] specifies *high-assurance systems*, also known as trustworthy systems. These systems are designed from first principles to be free of flaws. These include flaws 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 that face many of the same challenges (correctness, security, usability, accessibility, etc.) and

[2] 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

use the same technologies (operating systems, programming languages, distributed systems, cryptography, etc.) required by election systems. Our development process and methodology—cited prominently in NIST Interagency Report 8151,[3] 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 election systems and services market, at low cost, and with publicly owned open source technology on COTS hardware.

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.
- **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 US government.
- **Software Analysis Workbench (SAW):** Toolset to help scientists and engineers formally verify computer programs and establish provable correctness and security guarantees. Deployed by Amazon to provably guarantee the correctness of encryption software.

[3] NIST Interagency Report 8151: *Dramatically Reducing Software Vulnerabilities,* https://doi.org/10.6028/NIST.IR.8151

3.2 Vendor Customer Reference

We describe below projects that show our relevant experience, and also mention some of our clients that can act as references.

Software projects illustrating our relevant experience

Duration of Project Type	Project Description	Dollar Value
4 years	**High Assurance Cyber Military Systems (HACMS**). 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. 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	**Copilot.** 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	**Cryptol.** Funded by the NSA's Trusted Systems Research Group, Cryptol is an advanced tool suite for creating and verifying	>$10M

	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. In 2014, we made Cryptol publicly available and Open Source, with continued development taking the same approach as VSAP development proposed here. Cryptol is a prime example of our proven success in deploying and maintaining highly advanced technology.	
6 years	**Software Analysis Workbench (SAW).** 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	**CyberChaff.** 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 into their own products. The software is another good example of our capability to deploy and support advanced technology.	$1.2M

1 year	**Amazon s2n.** 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. 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 s2n code, our tools are run to make sure the changes are correct. 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 then provided Amazon with software that automatically scrapes the continuous integration logs to display easily-digested statistics about the success of test runs and the progress that had been made.	$800K

Hardware projects illustrating our relevant experience

Duration of Project Type	Project Description	Dollar Value
8 months	**SHAVE**. 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.	$500K

	Such a device is comparable to the "bump-in-wire" encryption devices deployed today within the DoD, 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.	
18 months	**GULPHAAC.** 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 also the world's first asynchronous (clockless) crypto chip. The chip operates at threshold voltage; it is extremely low power and low energy, and is energy-competitive with the lowest energy devices ever invented. The chip is power invariant, so if provided with 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.	$700K
4 months	**Undisclosed Client.** Free & Fair principals were responsible for performing a hardware and software quality and security audit of an authentication system that was meant to be used by members of the intelligence community in the field.	$90K

Customer references, including a characterization of the related project

Project Reference #1

Location: Washington, DC	**Date(s) of Work:** Mar 2015 - Sep 2016
Description of Goods and Services:	
Private Elections Quality and Security Audits 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.	
Reference Contact Information:	
Company Name:	US Department of Labor
Contact Full Name:	Tambra Leonard
Contact Mailing Address:	200 Constitution Avenue NW, Suite N-2474 Washington DC 20210
Contact Email Address:	leonard.tambra@dol.gov
Contact Telephone Number	+1 (202) 693-5744

Project Reference #2

Location: Portland, OR	**Date(s) of Work:** Nov 2015 - Mar 2016
Description of Goods and Services:	
C11 Verification Technology 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.	
Reference Contact Information:	
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

Project Reference #3

Location: Portland, OR	**Date(s) of Work:** Mar 2015 - Oct 2016
Description of Goods and Services:	
Galois Ultra Low Power High Assurance Asynchronous Cryptography Within this project, Free & Fair principals invented 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 also the world's first asynchronous (clockless) crypto chip. The chip operates at threshold voltage; it is extremely low power and low energy, and is energy-competitive with the lowest energy devices ever invented. The chip is power invariant, so if provided with 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.	
Reference Contact Information:	
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
Contract Telephone Number	(443) 634-3936

Project Reference #4

Location: Portland, OR	**Date(s) of Work:** Jun 2014 - Jul 2015
Description of Goods and Services:	
Future of Voting 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. This report is now the de facto reference for all R&D in internet voting.	
Reference Contact Information:	
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
Contract Telephone Number	+49 (0) 89 64939133

Project Reference #5

Location: Portland, OR	**Date(s) of Work:** Sept 2014 - present
Description of Goods and Services:	
SHAVE 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 DoD, 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.	
Reference Contact Information:	
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
Contract Telephone Number	+1 (703) 526-2886 ext. 2886

4.0 Products and Services Offerings

Table 1. Respondent's Interest in VSAP Components

VSAP Component	Expectations	Please Indicate if Interested in Providing
Vote By Mail	§ The software development of the Vote By Mail ballot design and layout, and the interfacing with the Elections Management System (EMS). § Certification by the California Secretary of State (shared responsibility).	Yes
Interactive Sample Ballot	§ The development and implementation of the Interactive Sample Ballot software. § Certification by the California Secretary of State (shared responsibility).	Yes
Ballot Marking Device	§ The development, manufacturing, assembly and implementation of the Ballot Marking Device software and hardware according to the design. This includes the privacy screen, the stand as well as the carrying case). § Certification by the California Secretary of State (shared responsibility).	Yes
Tally System	§ Review and incorporate developed Tally System software prototype into a production solution. § The procurement of scanners and interfacing those scanners with the Tally System. § Certification by the California Secretary of State (shared responsibility).	Yes
Thermal Printers	§ The printers necessary for the ePollbooks and the interfacing of them. § (Certification by the CA SOS (shared responsibility) and interfacing with the ePollbook and BMD.	Yes

Maintenance and Support	§ Ongoing Maintenance and Support of all software and hardware components listed above. § Continued upgrade of all software components. § Servicing and repair of BMDs.	Yes
Systems Integrator	§ The prime vendor who will be responsible for overseeing the overall implementation of the VSAP components listed above.	Yes

In the space below, please describe the products and services offered by the Respondent as applicable to the needs of VSAP as stated in the RFI. The following narrative should provide LA County with a general understanding of how the Respondent will be able to deliver the products and/or services marked in Table 3 above.

We will highlight our product offerings and services below, especially those that differentiate us from any other vendor in the world.

Products

We already have product demonstrators for several systems that operate like VSAP components. Most of these product demonstrators are high assurance. All are open source and available on our GitHub page.[4]

They are:

- a vote by mail system that is capable of understanding, interpreting, and helping adjudicate digital scans of paper ballots into cast vote records,
- a remote ballot distribution and marking system,
- a supervised voting system that includes an electronic poll book, a touchscreen-based ballot marking device, a smart ballot box, and a risk-limiting audit system, and
- a tabulator capable of consuming a plurality election's description, including cast vote records, and computing its outcome.

In addition to components that operate like those in the desired VSAP system, we have the following product demonstrators under development:

- an electronic poll book,
- a tabulator capable of tallying several non-plurality election schemes, including ranked choice voting, the Danish list-based scheme, the Dutch list-based scheme, and Ireland's proportional representation through single transferable vote (PR-STV) scheme,
- a polling place wait tracker that observes radio signals in a privacy-preserving fashion and deduces and publishes wait times for election administrators and the public, and

[4] See https://github.com/FreeAndFair for more information.

- a risk-limiting audit system that facilitates polling place or precinct-based ballot comparison audits.

We also have a large number of other technologies already developed whose goal is to help ensure the quality, correctness, and security of all of our election systems. These include, for example:

- an election test generator capable of generating all possible election outcomes for several complex election schemes, and
- a large set of tools that facilitate, and have been used for, rigorous systems engineering of high assurance election systems.

Services

We also offer a number of services that complement our product offerings.

They include:

- high assurance systems development, delivery, and support,
- the facilitation of high assurance systems certification (e.g., FIPS and Common Criteria),
- performing remote or on-site election auditing, including digital forensics of election equipment for criminal investigations, independent ballot interpretation or tabulation, election log analysis, and various forms of classical and new generation election audits, including risk-limiting audits, and
- training in advanced election concepts and technologies, including software independence, election cybersecurity, and risk-limiting audits.

Project Management Practices

In this section we review Free & Fair's project management practices, which we have used to deliver millions of dollars worth of high assurance systems on time and under budget. 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 to others at Free & Fair. 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 between 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 (in this case, Los Angeles 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.

Project Management Specifics for L.A.

Free & Fair is the prime contractor that will bid on the RFP. We have several subcontractors already arranged for the bid, all of whom are world-class entities whose expertise and focus areas complement our own. In particular, to complement our deep experience in high assurance software systems design and development, we have a hardware design firm with expertise in secure consumer hardware, a user-experience and user-interface firm with expertise in election systems and security, and a cryptography firm with experience in election technology.

5.0 Vendor's Proposed Approach to the VSAP Implementation

5.1 Ongoing Maintenance and Support

RR/CC is considering including ongoing maintenance and support services in a solicitation for the selected vendor (and its subcontractors). RR/CC sees that approach as creating a partnership with the vendor to help ensure the success of the entire project, however, RR/CC is seeking input from the vendor community on this approach.

1. Would you be willing to provide the County ongoing maintenance and support services for the VSAP solution for a specified number of years? What would be an acceptable, minimum number of years?

Yes, Free & Fair would be willing to provide the County ongoing maintenance and support services for the VSAP solution for a specified number of years. We require no minimum number of years.

2. Would having an agreement with RR/CC for ongoing maintenance and support be an incentive to you in promoting the VSAP solution to other jurisdictions even though you would hold no IP license for it, but would have significant expertise and commitment to its success?

Free & Fair measures our success not only by our financial bottom line, but also by the social impact of our work. Free & Fair's mission is to bring open source, high-assurance, end-to-end verifiable elections to the world. Thus, whether or not we had an ongoing maintenance and support agreement with RR/CC, we would work to promote the VSAP solution to other jurisdictions.

3. What, if any, alternative approaches to ongoing maintenance and support do you see and in what ways would they be better for you, RR/CC and other jurisdictions?

Free & Fair believes that RR/CC and other jurisdictions will be best served by competition in the market for ongoing maintenance and support, and by the option to privilege local providers. We offer ongoing maintenance and support to ensure that clients will have at least one high-quality option; at the same time we hope to see many other vendors offer this service to strengthen the business ecosystem around open source election technology.

5.2 Thermal Printer Requirements

The VSAP design includes the use of thermal printers in two instances (integrated with a ballot activation device (e.g., ePollbook) and embedded in the BMD). Thermal printing was selected primarily for reliability and the absence of ink and ink wells. However, there are three requirements of the design that exceed any known thermal printing product, namely:

- the paper size (8” x 11” and 8” x 13.25”)
- the paper thickness (143 µm).
- the paper must be thermal on one-side only, as the reverse side will be used to inkjet a Ballot ID, in 1-D human readable barcode format, onto the ballot prior to tally.

1. What solutions do you foresee for resolving this issue?

We do not see this issue as being difficult to resolve for existing thermal printer manufacturers.

2. What alternatives might there be?

Existing thermal printers from multiple manufacturers are capable of printing 8” wide paper at arbitrary lengths and at the thickness required by VSAP. The problem with existing off-the-shelf printers is that their form factors do not permit them to be easily integrated into the VSAP device. However, the internal mechanisms of such printers should be easily adaptable by their manufacturers for use in the VSAP device.

3. What manufacturers of printers would you foresee as helping or assisting you in integrating the VSAP solution and why?

We see both Brother, the leading manufacturer of large-page thermal printers for police and similar applications, and Fujitsu, who implemented the thermal printer for the VSAP prototype, as viable printer manufacturers for the final VSAP devices.

5.3 Potential Partnership Model for VSAP

5. RR/CC believes the best approach to VSAP is to have a strong Systems Integrator with specialized subcontractors. Please describe and include a graphical depiction of how the team may be structured, and what role you would hold.

We have worked with traditional systems integrators in the past on many projects. Our experiences with them are decidedly mixed, given their traditional operational and business models. Consequently, we have mixed feelings about the idea of having to work with such an integrator on the RR/CC project if we were to bid and win on any of the specialized VSAP components. As such, especially given our long experience in providing project leadership and integrator roles in R&D projects with the federal government, we will be bidding on the integrator role as well.

Our primary reflection in this regard is that RR/CC should ensure that the RFP not only allows such an arrangement (a company acting as both VSAP component developer and integrator), and also recognizes the strength in such a dual/multi-way offering, particularly if that company has the experience that we do in election technology and multi-institution/corporation project management.

6. Given your understanding of the County's goals and its priorities, what is your recommended approach to help the County achieve the following?

a. The retention of public trust in the voting system.

To build and retain public trust in a voting system, stakeholders must have a variety of ways to test the system. Individual voters, candidates, parties, public interest watchdog groups, election administrators and elected officials all have incentives to do so. Specifically, we recommend:

- Open source system design (including open source design of any non-COTS components), which allows election administrators and others to engage security experts to test the design.
- Open data formats for any data collected or exchanged by components of the systems. Ideally these data should be in standardized formats. NIST is currently working on creating data format standards for election systems data, and we recommend adhering to these eventual standards (unless other standards become more widely adopted).
- Mechanisms for election administration audits of the performance of the system in the actual election, starting from voter-verified paper records of voter intent. Risk-limiting audits are such a mechanism.
- Mechanisms for individual voters to test the ability of the system to record a single vote as intended by the voter. Cryptographic systems such as End-to-End Verification can accomplish this.
- Mechanisms allowing outside organizations of voters to compare information about Cast Vote Records with information about the final count. End-to-End Verification can accomplish this.

b. The adoption of the voting system by other jurisdictions.

We recommend:

- Well-advertised, transparent pricing.
- Good, well-funded storytelling both about the opportunity itself and the advantages of open source systems and evidence-based elections, as well as rebuttal of any prevalent misinformation, aimed at decision-makers in other jurisdictions.
- A Virtual Reality version of the polling place and election administration experiences to allow jurisdiction decision-makers (and existing and potential stakeholders) to get a feel for the system from anywhere in the world.

- Collaboration with academic and not-for-profit organizations with a national footprint, a track record of work in elections, and resources to promote information about VSAP.

c. Incentivizing the Systems Integrator beyond “work for hire” (payment for work performed) considering that the County will retain the software Intellectual Property (IP) of the components in scope for VSAP.

We recommend either choosing a different IP scheme (see response to Question 5 in Section 5.5) or providing royalties.

5.4 Certification

1. Have you had experience in working with a public sector Certification Agency to test and certify a solution? If so, please describe.

Our experience with certification comes mainly in the form of our past work in (1) facilitating the federal certification of cryptographic modules, and (2) providing consultancy expertise in the certification of high assurance systems against international standards such as Common Criteria.

With regards to our specific technical work, we expect to cut certification times in half or better by providing design, code, validation and verification artifacts immediately to the certifying 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 Free & Fair CEO Dr. Kiniry for use by The Netherlands in the 2004 European Council Elections. This high assurance 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.

2. How similar was that experience to the certification process outlined in the State of California Voting System Standards? See http://admin.cdn.sos.ca.gov/regulations/elections/california-voting-system-standards.pdf

The kind of certification work that we have done in the past is of a decidedly different nature—enormously more rigorous and exacting—than that which is mandated by the State of California.

We also have deep knowledge of election system standards, primarily via our direct contributions to the forthcoming VVSG 2.0 federal standards. Our contributions so far have been in rigorous systems engineering expertise, international elections expertise, case study

development, open source implementations of open data standards, cryptography and systems security, and more.

3. What issues or concerns do you foresee regarding certification of voting systems in California and what steps could RR/CC take to address them?

Our primary concern is the level of familiarity today's Voting System Test Laboratories (VSTLs) have with 21st century systems design and development concepts, processes, methodologies, tools, and techniques. These companies have been contracted for years to perform VVSG-based certifications that are based upon outdated procedures focusing on process, rather than artifacts—procedures widely rejected in the rigorous engineering systems community since the 1990s.

Consequently, if VVSG 2.0 evolves toward an artifact-centric approach to certification, we will have a dearth of VSTLs capable of performing efficient certifications. We have been working a bit with one VSTL to improve their capabilities to align with where VVSG 2.0 is heading, as well as to help them be more efficient and rigorous in their assessment of today's election systems.

We hope that California looks to where the VVSG 2.0 standard is heading so that their certification scheme will lead the way in ensuring that certification has a practical, measurable meaning with regard to the quality and security of certified systems.

4. As mentioned in the RFI, RR/CC is in progress on prototyping new ECBMS functionality related to the ballot layout and software for the new Tally System. A selected vendor may be required, as part of the contract, to review and revise the developed prototype, provide the necessary documentation, and be responsible for certification of the new Tally System by the Secretary of State. What issues or concerns do you have regarding this approach?

We welcome the opportunity to do this work.

5.5 Intellectual Property (IP)

The County is currently expecting the following IP to result from VSAP. The County intends to protect and license this IP:

- § Design for Interactive Sample Ballot (ISB)
- § Software developed for ISB
- § Design for Ballot Marking Device (BMD)
- § Software developed for BMD

§ Design for Vote By Mail (VBM)	§ Software developed for VBM
§ Design for Tally System	§ Software developed for Tally System

Additionally, the County does intend to protect its IP for the BMD hardware as an integrated device. The County does not intend to retain the IP created for component hardware that may be developed for the VSAP solution, such as a new version of a thermal printer.

1. Have you had experience in developing software using any form of open source licensing or disclosing and transferring source code to the public domain? If so, please describe.

Free & Fair has developed open source software, disclosed source code, and transferred source code to the public domain. As mentioned earlier in this document, in aggregate, we have 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).

Visit our two main GitHub Organizations to witness the millions of lines of open source code that we have released and support.[5] Individuals who work for Free & Fair have dozens of other open source projects scattered around the web, some of which go back to the early 1990s.

2. Whether you have or have not had experience in developing software under an open source license, what issues or concerns do you foresee for VSAP and what steps could RR/CC take to address them?

See response to Question 5.

[5] See the Galois GitHub webpage at https://github.com/GaloisInc/ and the Free & Fair GitHub webpage at https://github.com/FreeAndFair.

3. Have you had experience in developing IP on behalf of a public sector agency? If so, please describe including the details of ownership, cost and revenue sharing approach, and licensing conditions.

See response to Question 5.

4. Whether you have or have not had experience in developing IP on behalf of a public sector agency, what issues or concerns do you foresee for VSAP and what steps could RR/CC take to address them?

See response to Question 5.

5. Would you be interested in developing components of VSAP in a "work for hire" arrangement in which you were paid for the work performed but retained no IP of it? What issues or concerns do you foresee under this arrangement for VSAP and what incentives could RR/CC provide that would address them?

Yes, we would be interested in developing components of VSAP in a "work for hire" arrangement. However, we feel that Los Angeles County could not only save money but also contribute to the long-term health of the VSAP system by choosing a different IP regime.

The IP regime Los Angeles County advocates for in a full RFP will be a key factor in determining how many parties will submit proposals. Realizing the admirable goals of the VSAP system will require rare, highly-skilled technical expertise that is not available in standard IT consultancies, web development shops, and existing election vendors. Firms of this nature rarely engage in contracts where their services are provided as "work for hire" with full transfer of IP rights to the client, especially when significant research work is involved in the effort. If Los Angeles County requires such a transfer of rights, many qualified firms may opt not to respond.

For those that choose to submit a proposal, we expect that the cost of those proposals will be several times more expensive than if the system in question were to be made available under an alternative IP framing.

In addition, a healthy ecosystem of developers and users is essential to support Los Angeles County's vision of open source election technology shared by several jurisdictions and modified over time in response to law and practice.

We believe that Los Angeles County could meet the goals enumerated in the RFI by allowing an IP regime that includes joint ownership and long-term remuneration of all parties involved in the creation of the VSAP system. Thus, one of the two IP regimes described in the following paragraphs may be preferable to having Los Angeles County retain all IP rights.

Variant #1: Consortium Copyright, Licensed Certification Scheme, Election-centric License, Backend Financing

This variant would be more acceptable to potential vendors and we expect that the development cost of the system will be significantly lower. This position is aligned with best practices in commercial Open Source product development and maintenance where a product or platform has the potential for long-term, high-impact deployment and use. Examples of such a scheme include the ecosystems around the Linux operating system, the Java platform, the MySQL database, the Apache web server, Google Protocol Buffers, the OpenSSL cryptography library, and the Eclipse Integrated Development Environment.

1. Create a VSAP 501(c)(3) not-for-profit foundation, akin to the Linux, Apache, or OpenSSL Foundations. Ensure that membership in the Foundation is open to all who share the goals of Los Angeles County and VSAP, including the firm that develops the reference and deployed systems and deployment organizations such as value-added resellers, integrators, consultancies, etc. who build business models around VSAP.
2. Use a licensed certification scheme to enforce the VSAP trademark. By providing a reference implementation, subsystem behavioral interface specifications, and an automated means by which a third party can check the conformance of a new implementation (derivative or otherwise), the design conformance can be guaranteed and trademark use can be enforced.
3. Release the system under an Open Source Initiative (OSI)-approved license that is amenable to public use and adoption, such as the OSET Public License. Licenses such as BSD, MIT, or Apache are also possibilities. Each is broadly accepted and include few encumbrances.
4. Provide reasonable royalties to the organization that develops the original reference and deployed systems.
5. Prohibit awardees or any company that produces variants of the VSAP system from asserting any patent rights via contract.

Variant #2: Copyright Retained by Awardee, Licensed Certification Scheme, Non-exclusive License

This variant will be more appealing to vendors as well and follows the IP regime used by the Federal Government for research and development efforts.

1. The awardee that develops the system retains ownership of the copyright for all of their work. Los Angeles County and its subcontractors (such as the co-inventors of the VSAP system definition itself) retain copyright ownership for all of their work. Work that is performed jointly by Los Angeles County, its subcontractors, and the awardee is jointly owned by the participants.

2. As in Variant #1, introduce a licensed certification scheme to enforce design conformance and the VSAP trademark.
3. The awardee grants a non-exclusive, non-revocable, perpetual unrestricted license for the VSAP implementation and all associated artifacts developed under the course of the project to Los Angeles County.
4. The awardee's contract with Los Angeles County requires the following:
    a. awardee will make current and future versions of VSAP available to other jurisdictions on a RAND basis using a simple, clear, straightforward cost scheme that is mutually agreed upon by the awardee and Los Angeles County,
    b. awardee will release the system under an OSI-approved license that is mutually agreed upon by the awardee and Los Angeles County, and
    c. awardee will not assert any patent rights.

If Los Angeles County decides to retain the IP, we make the following concrete suggestions.

1. Ask the vendor to make a full transfer of copyright to Los Angeles County so that copyright protection is in the hands of a single entity. Copyright should be explicitly stated on all development artifacts including source code, specifications, developer and user documentation, etc.
2. Issue the system under the GPL version 3 license as it (a) forces derivative works and improvements in deployed products to be provided back to Los Angeles County, and (b) prevents the use of patents from forcing the code to be non-free.

Data Ownership

Matters relating to the ownership of data are much more straightforward, as we believe that election data produced by and for an election client, no matter where or how that data is housed, generated, or codified, should be owned by the client. No additional costs whatsoever should be imposed for access to, or trivial manipulation of, that data. Also, data should be protected by both copyright and licenses like all other artifacts associated with an open source system such as VSAP. Our favorite licenses for such are Creative Commons licenses.[6]

Intellectual Property Framing

We suggest that IP protection should be motivated toward framing business models for vendors and the client rather than matters relating to system design integrity.

We presume that design integrity means long-term design conformance. That is, a vendor must be unable to fork incompatible variants of VSAP and call it VSAP. This goal can be fulfilled by appropriate use of copyright and existing license law. A consortium of entities, whether it includes non-government entities or not, can enforce design conformance at least as well as a single entity can, and likely can do better.

[6] See http://creativecommons.org/ for more information.

Intellectual Property Design Decisions

We explain in the following our thoughts on design decisions about IP—decisions that must be made about several orthogonal dimensions, including (1) expression and protection of ownership, (2) transfer and restriction of rights of use and modification, (3) avoiding legal encumbrances, and (4) backend finances.

Copyright Transfer

Should copyright be solely or mutually held, and by whom? The obvious choices are (a) full explicit copyright transfer to Los Angeles County or some Consortium, akin to what is done at the Free Software Foundation (FSF), (b) mutual copyright is held between the organizations that develops the VSAP system, akin to what is done with regard to technology development at most universities and some companies in the USA, or (c) copyright is held by the original company that develops the VSAP system and rights to use, relicensing, etc. are all derived not from copyright ownership, but from licensing terms between Los Angeles County and the development organization.

License Choice

What kind of license or licenses should be applied to artifacts related to VSAP? With regard to matters of Open Source technology, the Open Source Initiative (OSI) is the main arbiter of license classification and community acceptance. Consequently, using an OSI-approved license is a wise choice. Ensuring that non-development artifacts are appropriately licensed is important as well. We prefer Creative Commons licenses.

Patent Avoidance

How can Los Angeles County avoid encroaching upon existing patents as well as avoid having other organizations improperly patent aspects of VSAP and thereby make VSAP non-free? The simplest means by which to achieve this goal is to adopt the GPL version 3 license for the system, as it contains clauses specifically addressing this concern. Alternatively, Los Angeles County can stipulate, via license and contract, that no patent rights can be asserted by either the winners of the RFP or any company that produces variants of VSAP.

Finances

Obviously finances will have a major effect with regard to the IP scheme chosen by Los Angeles County. Consequently, such choices will increase or decrease the number of proposers for any RFP.

As mentioned previously, Foundation schemes are not uncommon in the commercial Open Source space. Major operating systems, development platforms, and system components have been successfully developed and supported for decades using such structures.

We believe that both variants we summarize above hit slightly different “sweet spots” with regard to addressing the key concerns of Los Angeles County and ensuring that RFP responses are less expensive than outright replacing aging equipment with traditional vendor technology.

6. As the Systems Integrator of the VSAP solution, what incentives would you recommend the County provide you to build the best possible system and enable you to see yourself as a partner with the County in spreading the adoption of the system to other jurisdictions?

The best road to partnership would be an alternate IP scheme. For more information, see response to Question 5.

7. If the County IP License included a clause making it "forever free" software (which prevented it from ever being proprietary), what would you, as the developer, find sufficient to incentivize you beyond "work for hire"?

See response to Question 5.

8. Would you consider a Dual Licensing arrangement of the IP in which you, as the developer, had some exclusive rights not provided to anyone else? While still retaining the Open Source availability to all other entities, what exclusive rights would you consider minimal in your license?

See response to Question 5.

9. What form of Open Source licenses are you familiar with? Have you used any of them previously? Which one would you recommend for the VSAP solution and why? GPL? OPL? MPL? BSD? AL2? Other?

We have used a wide variety of Open Source licenses and are familiar with many more. For VSAP with IP owned by Los Angeles County we recommend GPL Version 3. Los Angeles may also want to consider the OSET Public License, an OSI-accredited license developed specifically for open source election technology.[7]

[7] See http://www.osetfoundation.org/public-license for more information about the OSET Public License.

5.6 Offshore Development

As indicated in the RFI, RR/CC is aware of the increasing degree to which firms have software and even hardware development offshore. Given the unique character of the VSAP products and their intimate relationship to the electoral process, RR/CC must ensure that public trust is maintained in the system. Additionally, the County may have legal restrictions related to offshore development and services.

1. Would a prohibition of offshore development of software in the VSAP solicitation be a concern to you?

No.

a. Would it raise the cost charged by you to RR/CC?

No.

b. What suggestions would you make to RR/CC regarding this issue?

Mandating that the VSAP system is developed onshore will likely lead to fewer bidders on VSAP components and most costly bids from traditional vendors. We believe that, if offshore development takes place, there should be full transparency about the location and nature of those developers, including their nationality, location, experience, salaries, etc. We presume that RR/CC want not only a system that voters can trust, but also one that was not delivered via unethical business operations.

2. Would a prohibition of offshore development of hardware in the VSAP solicitation be a concern to you?

Low-cost hardware manufacturing is dominated by firms in southeast Asia. While it is certainly possible to do all hardware design and manufacturing in the U.S.A., there are fewer firms with these capabilities and the final price of the resulting system will likely be significantly higher.

We understand the potential concerns with offshore hardware development—we are, in fact, performing on Department of Defense programs directly focused on the security concerns inherent with having hardware developed or sourced from untrustworthy overseas entities. However, we must note that these core concerns are not mitigated by simply demanding that hardware be developed onshore. We would be concerned if the prohibition of offshore development created a false sense of security.

a. Would it raise the cost charged by you to RR/CC?

It would very likely raise the per-unit cost of VSAP system hardware, which we would pass through to the County.

b. What suggestions would you make to RR/CC regarding this issue?

To address insider attack concerns, RR/CC should focus on:

1. the core security components of the VSAP systems (primarily the appropriate, transparent use of hardware roots of trust and cryptographically-based, academically-vetted means by which to certify that a system's provenance and attestation is as expected by the authorities), and
2. demanding that the VSAP system be software independent[8] and designed and developed around an end-to-end verifiable cryptographic protocol.[9]

If the core concerns focus on system quality or politics, we have no comment.

7.0 Pricing Information

We are not providing pricing information at this time, as final pricing will be highly dependent on the actual RFP requirements.

However, we expect to price our VSAP proposal using the same principles as in prior proposals we have submitted to other governments and organizations. We encourage RR/CC to examine those proposals, which are available in the Free & Fair Transparency repository on GitHub.[10]

[8] See "On the notion of "software independence" in voting systems" by Rivest and Wack to learn more about software independent voting systems. https://people.csail.mit.edu/rivest/pubs/RW06.pdf

[9] There are numerous end-to-end verifiable voting systems in the literature, including Scantegrity, Remotegrity, Helios, Zeus, DEMOS, Prêt à Voter, and STAR-Vote. We suggest that STAR-Vote is the appropriate system on which to base VSAP.

[10] https://github.com/FreeAndFair/Transparency