Response to The City and County of San Francisco's Voting System Request for Information

RFI# REG2015-01

Dr. Joe Kiniry, Galois, Inc., kiniry@galois.com

A. Summary Statements of Proposed System and References

1 Provide organization's or firm's legal name and address.

Galois, Inc., 421 SW Sixth Avenue, Suite 300, Portland, OR 97204

2 Provide the name, title, address, telephone number, and email address of the person(s) who will serve as the contact(s).

Jodee LeRoux, Contracts
Galois, Inc.
421 SW Sixth Avenue, Suite 300
Portland, OR 97204
phone 503.808.7209
contracts@galois.com

3 Provide a letter of introduction with a brief description of the organization or firm, including organizational structure, experience in the industry, number of years providing voting systems and election support services to federal, state, or local governments.

Galois is a privately held U.S.-owned and -operated company established in 1999. Our mission is to provide trustworthiness in critical systems. We were founded on core principles that focus on innovation, authenticity, and deep trust, and we live those principles every day in interactions with clients and among ourselves. We specialize in the research and development of new technologies that solve the most difficult problems in computer science. Our team works closely with clients to achieve a balance among the privacy/cost/speed challenges involved in making systems more trustworthy.

Galois has 60 employees in 2 offices (Portland, Oregon and Arlington, Virginia), with principal investigators leading research and engineering teams in the areas of cryptography, software correctness, mobile security, cyber physical systems, computer security, machine learning, human machine interaction, and scientific computing.

Galois has won and successfully executed on dozens of multi-year, multi-million dollar R&D projects for numerous federal agencies including the Department of Defense (DOD), the

Department of Homeland Security (DHS), Defense Advanced Research Projects Agency (DARPA), Department of Energy (DOE), NASA, and members of the Intelligence Community.

Galois has a fifteen-year proven track record of solving the most complex challenges of the most demanding federal and commercial customers. Our bespoke software products are internationally recognized as being some of the best technology in the world of high-assurance software systems. Consequently, we intend to fundamentally change the nature of elections systems design, development, and support and put the power back in the hands of the voting public.

Early in Galois's existence we recognized that democracy should be treated as a high-assurance system, so we have had a long-term interest in developing technology for elections. A high-assurance system, or trustworthy system, is a system 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 historically 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).

Historically, Galois has not executed on election systems. However, we have successfully developed many systems that have many of the same challenges (correctness, security, usability, accessibility, etc.) and technologies (operating systems, programming languages, distributed systems, cryptography, etc.). Thus, we are well positioned to bring the assurance one sees in other safety- and mission-critical high-assurance systems to the elections systems and services market, at low cost and with publicly owned open source technology on COTS hardware.

Galois has a flat, peer-to-peer organizational structure. Senior personnel who have national or international experience relevant to the development of elections systems include Dr. Joseph Kiniry (an internationally recognized expert in high-assurance systems, security, and elections), Ashish Puri (a nationally recognized expert in development and implementation state-level IT systems, including the design and development of HAVA compliant Voter Registration and Election Management systems), Harri Hursti (an international elections security expert, who has been infamously involved in several state-mandated deep audits of elections technology), Maggie MacAlpine (a national election processes and auditing expert), and Dr. Daniel Zimmerman (a former professor at two institutions and an internationally recognized expert in high-assurance systems design and development).

For the past year, we have been developing prototype technologies in this space that include an electronic poll book, a verifiable in-person voting system, and tabulation and auditing techniques that support ranked choice voting. We are in the process of spinning out a class B corporation, Verifiable Elections, whose mission is to bring open source, high-assurance, end-to-end verifiable elections to the world. This new company will be a Galois-branded entity and will retain much of the personality, history, technology, and performers of Galois. Dr. Kiniry is the

Chief Scientist and CEO of Verifiable Elections, and Dr. Zimmerman and Mr. Puri are key members of its management team.

Prior to working for Galois, Dr. Kiniry provided commercial and public consultancy services to several governments on matters relating to elections, their technology, security, processes, and verifiability. His experience in the area of elections is both from the perspective of a public employee (as he was a professor of computer science and mathematics at multiple universities for approximately twelve years) and as a scientist-activist. 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 electronic poll book systems); and sits on the Board of Advisors of the main verifiable elections nonprofit, Verified Voting.

Dr. Kiniry has formally advised three governments (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 U.S.A. He co-ran a multi-year research project on digital elections (the DemTech project) 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 electronic poll book system for Danish national elections.

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.

Ashish Puri is the Strategy and Client Engagement lead for Galois's state and local public sector vertical focused primarily on elections, and shares Dr. Kiniry's drive and passion for innovation and improvement in elections. Mr. Puri has worked in U.S. public sector delivery for over fourteen years, including the e-government elections vertical for twelve years, holding several key client and delivery roles for Hewlett Packard and its subsidiary companies. Mr. Puri was the lead elections SME for 9 statewide VREMS projects for HAVA compliance in various roles in analysis, design, product development, project, portfolio and practice management, culminating in his leadership of the Elections practice servicing 13 U.S. states at Saber Corp, a company that was acquired by EDS/HP. He brings deep understanding of the development and implementation of elections products. In addition to elections, he has managed key projects and practices in the areas of motor vehicles, child support, telecom, insurance, and health and human services.

Dr. Zimmerman, the Technology Lead at Verifiable Elections, has extensive experience in formal methods, high-assurance software engineering, concurrent and distributed systems, and foundations of computer science. Before coming to Galois, he taught computer science at multiple universities for over a decade. At Galois, he has worked primarily in the areas of rigorous software engineering and verifiable elections technology.

Harri Hursti has focused on uncovering data security problems in electronic voting systems globally. He has revealed severe problems in electronic voting systems worldwide, and is famously known for developing the Hursti Hack, in which he demonstrated how the voting results produced by the Diebold Election Systems, Inc. voting machines could be altered. Scientists from UC Berkeley, commissioned by California's Secretary of State, verified the Hursti Hack. HBO turned the Hursti Hack into a documentary called "Hacking Democracy", which was nominated for an Emmy award for outstanding investigative journalism. He has subsequently been involved with various academic studies on elections, including the EVEREST study commissioned by Secretary of State of Ohio.

Margaret MacAlpine, Auditing Specialist at Verifiable Elections, has managed risk limiting and transitive audits in Florida, Connecticut, and most recently in Colorado. She has served as an advisor of 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 election audits. She also contributed to the "Security Analysis of the Estonian Internet Voting System" in partnership with the University of Michigan.

In general, Galois's work, reputation, and way of doing business—based upon trustworthiness, authenticity, and transparency—means that virtually all our customers become repeat customers. Consequently, we are happy to introduce any potential client to any existing or past client as a referral. We provide some specific referrals herein.

4 Provide a summary of the products and services offered, including annual license fees, annual support fees, and/or annual subscription fees. Include third party applications that are being recommended. List prices are acceptable.

Galois is focused on building systems based on the concepts, foundations, tools, and technology of high-assurance systems engineering. We typically work on systems that must be completely free of bugs and security issues. Our elections systems are of the same ilk. Our portfolio of offerings includes all aspects of the voting process that require high assurance, from electronic poll books to post-election audits. Other aspects of our offerings include: ballot marking devices, verifiable vote-by-mail, independent ballot verification, ballot tabulation of both digital and paper ballots, advanced accessibility features, tracking of polling place line lengths, risk-limiting and full-election transitive audits, and complete election results verification using end-to-end verifiable technologies. Our products that support recording voter choice, tabulation, and full election audits support rank choice voting as per the requirements stipulated in this RFI.

Our primary goal in developing elections systems is to increase transparency and trustworthiness in the election process. Our products are all Open Source, customers can purchase fit-for-purpose versions, and we have a variety of support and service contracts. Our current pricing model is dependent upon populations served and involves no recurring costs. Customers own the products that they purchase and our licensing scheme is perpetual, not limited to a fixed time period.

We are committed to providing defect-free, high-assurance solutions to our customers. As part of this commitment, we provide a lifetime warranty on our software and fix any defects discovered for free and in a timely fashion rather than limiting such support to a particular time period under a maintenance contract.

5 Describe any election-related services that the organization or firm offers, including, without limitation, integration assistance, training, and ongoing support. Provide a rate structure or other costing information (i.e. hourly rate or pricing methodology) for the professional services offering. List prices are acceptable.

Galois recognizes that any system implementation not only requires a technically sound and robust product with comprehensive business functionality at its core, but also needs to be supported by professional services throughout the project life cycle. We have expertise in professional services such as project/program management, software design and development, testing, mentoring and training, implementation and go-live as well as post-implementation operational support services.

At Galois, we typically run a very lean ship when it comes to project management and customer caretaking. We can be lean because our research engineers are all 10x programmers, most of whom have PhDs, and because of our focus on trust and transparency in all business and technology.

For example, we use a model for service guarantees and operational support that is atypical because our systems are high-assurance and formally verified. Instead of a traditional triaged tiered support system, we provide a comprehensive support solution that emphasizes transparency about the product and its capabilities and direct access to the team responsible for the product.

For our traditional projects, customers have direct telephone and email access to the project lead, direct access to the project's ticket system, and direct visibility into the development repository of the project. Support tickets filed in the system are typically triaged by team members within minutes, responses to issues are immediate, and fixes are prioritized based on conversations between the customer and the development team. We can provide evidence of these claims by simply referring evaluators to our Open Source product repositories.

For field support during deployment and system use, we augment operational support with a front-line team that can provide basic support to election officials and volunteers. We plan to provide support of this kind via a toll-free number, an online text chat interface, online video chat support, or any combination of these.

We also provide training offerings related to our products; Open Source technology adoption, legality, and use; certifications; evolving national and international standards in elections technologies; and rigorous software development.

Despite the fact that our products are high-assurance and include a wide range of untraditional artifacts—such as formal specifications, tests, and proofs—to guarantee their correctness, security, usability, and accessibility, they are no more expensive than existing products. In fact, our methodology is intended to significantly decrease the cost and time of certification.

6 Describe the different implementation approaches (i.e. big bang vs. phased roll out) that the organization or firm can offer to the City to fully implement a particular solution. Include the benefits and/or risks of each.

At Galois, our personnel have extensive experience in system implementations based on different approaches including big bang and staggered or phased roll-out. A big bang approach, while sounding imposing in terms of the extensive implementation support effort that it may entail, is quite often the best way to proceed. However, extensive user and system testing in a production simulation environment like a model office or, in this case, a mock election must precede it.

A staggered or phased implementation approach is beneficial when there are multiple iterations of the same kind of activities across several sites, time is not a driving factor in the cutover, and there are no constraints on resource availability. An example of this could be replacing multiple systems with one system as was done for HAVA compliance when multiple county systems (sometimes up to 100) in a state were replaced by a single statewide system. Since similar data sources were being integrated into one single database, reusing the data conversion engine, improving and augmenting it with each set was a good option. The same could be said for the training courses and field support.

Based on the time constraints laid out in this RFI, with the expiration of the current support contract in December 2016 and the anticipated release of the RFP in early 2016, it seems that a big bang approach will be best for the city and county of San Francisco. We would recommend that the project have critical gates for conducting mock elections in some pilot locations (at least one if not two cycles) in addition to user and system acceptance testing to ensure that the system is ready for prime time for production cutover and live elections. The mock elections should be conducted over a good representative sample of the polling locations (at least 2–5) that cover variances in ballot size and complexity, multilingual ballots, accessibility needs, and other critical aspects of the voting process to ensure a wide-ranging test of actual election-day scenarios.

7 Provide a brief description of the overall software and architectural design of applicable products.

Our design and architecture for election-related systems is highly modular. Each module uses only open data formats for communication, resulting in a system that can be modified and upgraded by anyone who is familiar with the open standards that we use. This modular architecture features an air gap between the software responsible for running the election and the software for designing and reporting on it. A modular architecture assists with compositional validation and verification, experimentation with user experience variants, and 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 cryptographic foundations, ranging from authentication to data-at-rest to provenance-preserving logging, are based upon our work on another one of our products, Cryptol, and a host of advanced tools and technologies for academic partners and ourselves. In general, 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), custom formal protocol design and verification, custom formally verified cryptographic libraries, and logging with privacy-preserving cryptographic integrity.

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.

Software correctness is an integral part of the Galois development approach, beginning with the specification of a system's domain model, requirements, and software and network architecture. By formally specifying the initial design, and developing the implementation based on the resulting specification, we guarantee that we are implementing exactly the desired system. We also incorporate the vast majority (typically on the order of 99%) of the software tests within the code itself, rather than developing tests separately, and these tests are, for the most part, generated automatically from formal specifications. This leads to a software product built with quality inherent in its foundation, rather than with defects to be detected and fixed later. In addition to this pervasive testing, quality assurance is achieved through strict configuration management and systematic validation of the code as well as the all evidence-based artifacts and documentation produced.

For the most essential parts of the software we go a step further, performing a machine-checked functional verification of the software. In this process we first design a mathematical model that should be 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 any computer, giving unparalleled assurance that the software is correct. These techniques have historically only 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 approaches, we get a chain of correctness that starts with the high-level system specification and continues all the way 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 for example 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 artifacts that give external parties the same confidence in our software that we have.

The specific peer-reviewed methodology we use for all of our software is a variant of Design by Contract with some aspects of a Correctness by Construction approach. Our process, method, tools and technologies span several deployment and development platforms, specification and programming languages, and communication and coordination schemes.

8 Describe the recommended operating environment(s) required to install and use any relevant systems and the minimum system requirements necessary to run such systems. Include any suggested production, development/test, and disaster recovery environments.

Our software solution will be compatible with a variety of commercial off-the-shelf (COTS) hardware and operating systems. Voting terminals can be deployed on readily available laptops, tablets, and similar devices running on industry-standard operating systems, such as Microsoft Windows, Apple's OS X, Linux, and various versions of BSD UNIX. Likewise, the central election office computing systems used to design ballots, provision voting terminals, tally voted ballots, and perform audits can be deployed on readily available COTS hardware.

For extraordinary products, we are capable of designing, building, and verifying custom hardware (e.g., embedded microcontrollers that cost tens of dollars instead of thousands, and ARM and MIPS-based devices) and non-traditional operating systems (e.g., real-time operating systems such as those of Wind River Systems).

The system will have sufficient redundancy that no separate disaster recovery environment will be required.

Beyond computational requirements, we will provide guidelines for how to purchase and install systems in order to maximize security. Testing will be built into the software, and will not require additional hardware or a separate testing environment. As an optional service, we can select, purchase, configure and maintain appropriate hardware based on the specific needs of San Francisco County.

9 Describe how the organization or firm envisions its software and hardware solutions changing over the next five to ten years.

We expect that our software offerings will evolve as customer demand for new applications and services evolves. Our hardware offerings will be predominantly COTS, with very little custom hardware, and all our custom hardware will be developed as Open Source. While we are performing R&D on new products and Internet-based services, we would rather not read the tea leaves of future elections customers to predict which of those efforts will result in product offerings.

We expect that our current offerings will continue to evolve, but only as demanded by customers, by certification, and by law. We do not expect our products to explode from a fine-tuned set of features to over-bloated software, as we have witnessed in so many mainstream and election systems products.

Our software products will continue to be Open Source, continue to include evidence of their certification, correctness, security, usability, and accessibility, and continue to be cross-platform and run on COTS software and COTS and Open Source hardware. We will continue to provide a lifetime warranty on our software and fix any defects discovered for free.

We expect that, based upon historical precedent, COTS and Open Source hardware that fulfills the minimal requirements mandated by our Open Source software and certification will decrease in cost from year to year, thereby decreasing the overall cost of elections.

Over this time frame we also expect to see a flowering of local support vendors and integrators come into existence whose focus is on Verifiable Elections technologies, much as we have witnessed over the past two decades for Linux and other major Open Source platforms.

10 If applicable, submit at least two (2) references of federal, state or local governments equal in size or larger than the City and County of San Francisco that have implemented the proposed system, or, a similar system, within the last five (5) years.

The following three projects are at the forefront of R&D in topics of direct relevance to election systems, primarily the correctness and security of cyber physical systems, the cryptography in secure systems, and next-generation elections.

Name of Client: DARPA
Contact: Dr. Kathleen Fisher, Tufts University, ph 973.610.2668, kfisher@eecs.tufts.edu
Date: ongoing with major deliverables already complete
Employees: 1,000+
Project: Our work for DARPA is in the context of the HACMS program which focuses on high-assurance cyber physical systems. Cyber physical systems (CPS) are basically "computers that control things that have a physical manifestation", including planes, trains, automobiles, drones, etc. Voting systems also fall under this category. Galois had never worked in this safety-critical domain when we won this multi-year, multi-million dollar contract. We are now recognized as one of the top R&D entities in this field. This project is relevant because our results for HACMS were developed on COTS hardware and resulted in Open Source software and major changes in the way the government and industry think about the assurance of CPS.

Name of Client: Maryland Procurement Office
Contact: Dr. Sean Weaver, ph 443.634.3872, saweave@tycho.ncsc.mil
Date: ongoing with dozens of products and major deliverables complete
Employees: 1,000+
Project: Our work for the Department of Defense is primarily in the context of two systems: Cryptol and the Software Analysis Workbench (SAW). Cryptol is a programming and specification language that focuses on cryptography. SAW is a formal verification system that permits one to reason about the formal correctness of algorithms at the bit level. The U.S. federal government uses these tools for R&D on current and next generation cryptography for national security. This project is relevant because cryptography is a fundamental component of modern election systems and we are viewed by the federal government as being one of the top R&D firms in the world in this area, as evidenced by our fifteen years of contracts on this topic.

Name of Client: U.S. Vote Foundation
Date: early 2014-mid 2015
Employees: ~10
Contact: Susan Dzieduszycka-Suinat, +49 (0) 89 64939133 (note this is in Germany), susan@usvotefoundation.org
Project: Our work with the U.S. Vote Foundation is in the context of next-generation election systems. Galois was the technical lead on the End-to-End Verifiable Internet Voting (E2E-VIV) project, whose goal was to frame the discussion and future R&D on the controversial topic of Internet Voting. As a part of this project, high-assurance elections systems running on COTS hardware were developed and a book-length report was written that is now the foundation for all future work in this area. The federal government as well as numerous state and local election authorities, both in the U.S. and abroad, are now using this report.

Note: Reference below for work performed by Ashish Puri as Project Delivery Executive and Elections Practice Director at Saber, an HP company.

Name of Client: Colorado Secretary of State
Contact: Trevor Timmons, CIO, ph: 303.894.2200, Trevor.Timmons@SOS.STATE.CO.US
Date: 2007-2008
Employees: 100+
Project: CO SCORE II, implemented in 2007-2008, is a centralized statewide voter registration and election management system that was built to comply with HAVA. It replaced 64 counties' VR and EMS systems in Colorado and provided a collaborative platform for registration, setup and conduct of elections at the statewide or individual county level. It has interfaces with other agencies for voter validation and list cleanups and provides comprehensive data export capabilities for downstream functions, such as electronic poll books and voting and tabulation systems. The system is based on high availability architecture (HAA), with redundancy built in at every level and built on the .NET platform served over CITRIX with Oracle backend. It is accessible using a web browser for election officials and has some public facing modules.

B. Specific Criteria for New Voting System

We have reviewed the provided list of functional requirements in depth. All of the required functionality, except for one criterion that we discuss in detail below, is straightforward for Galois to implement; we also have one suggestion for strengthening the technical requirements. We are actively engaged with the California Secretary of State and intend to follow the guidelines under SB 360 to work towards certification of the proposed system. Our commitment to open source software with a focus on transparency, correctness, and accountability makes us comfortable with all criteria relating to testing, logging and reporting. Many of the open data formats used within the system will also be suitable for data export, and the modular nature of the system makes it easy to add automatic translation from these open formats to any other specific data formats required by the County.

Our only technical concern is with criterion 1.o., which requires auditing of ballot cards at multiple points during the tabulation process. Existing auditing techniques gain their statistical significance by selecting randomly from a complete body of ballots and continuing the audit process until thresholds related to the final results of the election are reached. For example, a close race requires a larger number of ballots to be audited than a race that is won by a large margin.

We are currently unaware of any risk-limiting audit techniques that are specifically designed to work with ranked choice voting systems. We believe that such techniques can be developed, but their development is a matter of scientific research rather than a straightforward implementation. Thus, the timeline for availability of these techniques is more unpredictable than that for the rest of the system. We have already begun this research with international experts in risk-limiting audits and election law.

We believe that the technical requirements could be strengthened with an additional criterion stating that any new voting system for the City and County of San Francisco must be end-to-end verifiable. End-to-end verifiability allows voters to check that their votes were correctly recorded and check that the voting system included their votes in the final tally, and also allows voters and independent observers to verify the accuracy of the final tally and election results. This can be achieved without compromising the privacy or security of the vote.

With respect to procurement mechanisms and costs, we strongly believe that counties should not be locked in to proprietary hardware solutions accompanied by costly lease arrangements and unnecessary recurring maintenance costs. As described above, our pricing model is dependent upon populations served and involves no recurring costs. Our products are Open Source, customers own the products that they purchase, and our licensing scheme is perpetual, not limited to a fixed time period. Our model promotes ownership of COTS hardware, which has a significantly lower cost than proprietary leased hardware and can, if desired, also be used for purposes other than election administration. As previously mentioned, we are flexible about the approach that works best for the City and can select, purchase, configure and maintain appropriate machines based on the specific needs of San Francisco County if desired.

Our team clearly understands the need for adaptability in the face of evolving elections legislation. We closely follow developments in this area and are well versed with the increasing reliance on mail ballot elections and vote centers. Our modular architecture is designed for adaptability, and our verifiable vote-by-mail offering can work either in conjunction with our in-person voting system or as a standalone system for early remote voting. This provides flexibility to adapt to the direction taken by the city and county of San Francisco in accordance with SB 450 or any other elections legislation that may come into effect.