FROZEN DOCUMENT

Electronic Poll Books

RFI # 7549913 - Galois Response

16 October 2015

Responder

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

Point of Contact

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

Company Profile

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. We have 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.). Our elections team brings together internationally-recognized technical and domain experts who are committed to improving democracy and its realization through e-government systems. 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), 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 is a key member 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 meant to be used in 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. Dr. Kiniry is a key actor in the newly formed NIST-EAC Public Working Groups.

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. The Hursti Hack was verified by scientists from UC Berkeley, commissioned by California's Secretary of State. 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.

Galois Verifiable Elections R&D

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,[1] and a host of advanced tools and technologies for ourselves and academic partners. 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.

[1] http://www.cryptol.net/

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 unparallelled assurance that the software is correct. These techniques have historically been used for safety-critical systems, where the failure of a system would result in loss of life (e.g., flight control systems at Airbus) or have enormous cost implications (e.g., failure of a mission to Mars).

By combining these 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[2] with some aspects of a Correctness by Construction[3] approach. Our process, method, tools and technologies span several deployment and development platforms, specification and programming languages, and communication and coordination schemes.

Support, Staffing, and Help Desk Services

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.

---

[2] https://en.wikipedia.org/wiki/Design_by_contract

[3] https://buildsecurityin.us-cert.gov/articles/knowledge/sdlc-process/correctness-by-construction

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.

Electronic Poll Book Requirements

The proposed electronic poll book system (hereafter, the system) satisfies all stipulated minimum requirements. In particular, in the order in which the requirements are listed in the RFI:

1. The system can accommodate an arbitrary number of devices, and is designed to be fully fault-tolerant; any devices that fail due to hardware malfunction, accidental damage, or other issues can be replaced on-the-spot by poll workers, without requiring technical support intervention and without compromising the security or integrity of election data.
2. The system allows poll workers to list, search, identify and authenticate voters by matching against partial or full names, partial or full addresses, or any other voter identification information available from Rhode Island's CVRS.
3. The system can verify the precinct assignment for any voter based on registration information or, in the case of voters for whom registration information is not available (who must vote provisionally), address information. It can also provide guidance (including maps and step-by-step directions) to the correct polling locations for voters who attempt to vote at incorrect locations.
4. The system logs detailed information about provisional ballots cast on Election Day, including the voter's personal information, the ballot style used, and why the voter was given a provisional ballot. This information is also available to election officials and propagated across the electronic poll book network in near real time, which prevents the distribution of multiple provisional ballots to voters who present the same identifying information.

5. The system will be compatible and work seamlessly with Rhode Island's CVRS, provided that the CVRS supports data import and export in some well-defined format or provides a well-defined access API for data access and updating. The actual compatibility layer between the system and Rhode Island's CVRS would be designed and developed after examination of the technical details of Rhode Island's CVRS.
6. The system is highly configurable and customizable in several dimensions, including appearance and conformance to local election laws.
7. The system prevents unauthorized access to and dissemination of sensitive or confidential voter information in the following ways:
    a. All events in the system—including searches, voter check-ins, ballot distributions, gathering of provisional voter data, and changes to registered voter data—are logged in a cryptographically secure and tamper-evident way. These secure logs are distributed across the electronic poll book network such that they are available to election officials in near real time; log information can survive the simultaneous loss of multiple electronic poll books, and any attempts to modify log information can be easily detected.
    b. All electronic poll books have built in tracking (either via GPS or Internet-based geolocation), can be disabled remotely by election officials, and can disable themselves in the event of unauthorized use. All sensitive or confidential information stored on the electronic poll books is encrypted at all times except when being prepared for display or printing, and only authorized users may cause information to be displayed or printed. All communication of any kind on the electronic poll book network is encrypted with transport layer security (TLS), and sensitive or confidential information is always transmitted in encrypted form.
8. The system can generate customizable activity and audit reports. This customization can be performed by election officials without the need for technical support involvement.
9. The system is extremely easy to set up and manage. It is user-friendly for voters, poll workers, and election officials alike. Its look and feel is "Google simple", with no unnecessary information or confusing options presented to a user at any step and built-in help always available.

The proposed system also fulfills all the additional features of interest. In particular, in the order in which the features are listed:

1. It is compatible with commercial off-the-shelf (COTS) magnetic strip and barcode readers for scanning voter driver's licenses or ID cards.
2. It is compatible with commercial off-the-shelf printers and dedicated ballot on-demand printers, for printing ballots, general election information, instructions to polling places, etc.
3. It can, as desired by election officials, include "FAQ" capability to help poll workers address voter questions regarding voting and Election Day procedures.
4. It can provide lists of voters matching any of the previously-mentioned search criteria, or lists of voters for particular precincts, to poll checkers.

Detailed System Information

In this section, we address the RFI's requests for detailed information about the proposed system and its capabilities. In the order requested:

1. The proposed electronic poll book system is software-only and runs on COTS hardware. There are no current or pending federal, state, or organizational certifications of our electronic poll book software.
2. The electronic poll book system includes all necessary software components. It is capable of running on a wide variety of COTS hardware and operating systems, including Android, iOS, Linux, Windows, and Mac OS X. We recommend the use of iPads or Android tablets as electronic poll books, as they are affordable, easy to provision and administer, and capable of directly accepting voter signatures on their touchscreens and directly scanning barcodes with their cameras (eliminating any need for separate signature pad and barcode scanning devices).

   The electronic poll books require Internet access for communication amongst themselves and live monitoring by election officials; this access can be provided using existing WiFi or wired connectivity in polling places, commodity LTE hotspot devices, or LTE capabilities built into the electronic poll books themselves. At each polling place, only one connection to the Internet (using a dedicated router or shared, "personal hotspot"-style, by a poll book) is needed, though more than one may be desired to provide resiliency in case of network failures or service disruptions.
3. The CVRS could be used by/connected to the electronic poll book system in one of two ways, depending on client preference:
   a. All necessary data would be exported from the CVRS before the election and loaded into the electronic poll book system. The data in the electronic poll book system would be modified during the course of the election, and the CVRS would be updated with the modified data after the election's completion. Both the export and import would be guided, but manual, operations; that is, election officials would run a data import/export application to export the data and convert it to the electronic poll book format, and later run the application again to review the changes and convert them back from the electronic poll book format to a format suitable for updating data in the CVRS.
   b. The electronic poll book system would access the CVRS using an API, and import data automatically before the start of the election. It would optionally be able to update its data during the election to reflect changes made to the CVRS data by election officials. If desired, the system could perform live updates to the CVRS during the election using the same API; however, our recommendation would be that updates to the CVRS should not occur live during the election, but only after the close of the election once election officials have reviewed the updates to be made.
4. The setup and configuration of the electronic poll book system is very simple. The system has a peer-to-peer architecture, so every unit in the system has exactly the same

software installed. One unit needs to be set up as the "initial" poll book; this poll book is supplied with the CVRS data (as described above) and election-specific information (dates, ballot styles, polling places in use, etc.). Additional poll books configure themselves automatically, needing only to be told what polling location they are to be used in, to be connected to the same local area network as an existing poll book (in which case they will discover the poll book system automatically) or given the Internet address of *any other poll book in the system*, and to be authenticated as part of the startup process. In practice, one or more poll books (to be used for election monitoring) would be placed in fixed locations, such as central election offices, with known Internet addresses; the first poll book to be powered on in each polling place would be supplied with the address of one of the fixed poll books, and subsequent poll books powered on in a polling place would either be supplied with a fixed poll book address or configure themselves automatically using the local network.

Because it is important to ensure that only authentic poll books are in use, every poll book must be properly configured and authenticated when it connects to the network. This process is traditionally done using passwords, but in the proposed system is dramatically simplified by using *Tozny*,[4] an Android and iOS app that permits secure authentication to devices and software without the use of passwords or even touching the devices in question. In short, when a poll worker authenticates herself to an electronic poll book on Election Day, she does so by pointing her mobile device's camera at the poll book's screen. Likewise, to configure a new poll book in a polling place, a poll worker simply points their camera first at an existing poll book's screen, then at the new poll book's screen. Finally, to close the polls at a polling place, once again the poll worker points her device's camera at a poll book's screen. This is a completely hands-off, trivial authentication procedure usable by even the computer averse or the disabled, and can be performed using any Android or iOS device with a camera and an Internet connection. In situations where poll workers do not have, or cannot be temporarily issued,[5] mobile devices to use during the election, passwords can still be used as an authentication mechanism.

5. Voter data is kept confidential and secure in two main ways: by being protected on the individual poll books, and by being protected when communicated over the Internet between poll books.
    a. Each individual poll book stores voter information in a local database, which has three layers of protection: first, access to the database is controlled via a local encrypted channel; second, the database is stored encrypted on the device; third, all sensitive data stored within the database is itself encrypted by the poll book software. Moreover, computation on sensitive data is performed *without decrypting the data*, so that no sensitive data is ever decrypted into clear text on disk, in memory, or on the network except for display and printing as part of poll

[4] http://www.tozny.com/

[5] It is straightforward to provide affordable Android devices, with no cellular plans or other ongoing costs, to be used for authentication during the election cycle by poll workers who do not have mobile devices of their own. Such devices cost well under $50 each and can be reused for multiple elections.

book operations. This security architecture means that, even if a malicious party steals a poll book and has administrator rights on its operating system and administrative access to the database software, they can obtain no sensitive information.

b. All communication within the peer-to-peer poll book network uses secure channels (TLS) to ensure communication integrity. Moreover, all data transmitted over the secure channels is encrypted and digitally signed, ensuring both integrity and authenticity of the data. Finally, the network protocol has been formally specified and verified for both correctness and security.

6. We previously described the initial configuration of the electronic poll books for the election and at the individual polling places (in (3) and (4), above). Once configured, each poll book is used according to the following procedures. Note that these procedures do not exactly correspond to the RFI's list (a)-(g) of "important steps to cover", though they do address all the issues raised in that list.
    a. The typical flow for signing a voter in to a polling place and distributing a ballot is as follows:
        i. The voter identifies herself to a poll worker in some manner that satisfies Rhode Island law.
        ii. The poll worker enters information about the voter into the electronic poll book, either by hand or by scanning the voter's ID with a barcode or magnetic strip scanner.
        iii. The poll book displays to the poll worker a list of all voters in the database with matching information and prompts the poll worker to select the correct voter; this can be determined by looking at additional pieces of identification, asking the voter to verify their address if they have not provided identification with address information, etc. If only a single voter matches the search criteria, as would be expected when scanning a voter's ID, this step is skipped. If no voters match, the system gives the poll worker the option to handle the voter using the provisional ballot process (described in (b), below). If information was entered by hand the poll worker can also return to step (ii) and start a new search, either to correct any data entry errors or to search using different pieces of identifying information (in case incorrect data was previously recorded in the CVRS).
        iv. The poll book displays information about the voter. If the voter's address changed 30 days or more before the election and their old address appears in the poll book, it can be updated by the poll worker at this time (assuming the voter has satisfactory legal documentation of the address change).
        v. The poll book displays up-to-date information about the voter's eligibility to vote in this election and, if the voter is in the correct polling place, reports the ballot style the voter should be given (including the special Limited Ballot, in appropriate situations). If the voter is inactive, or is otherwise ineligible to vote in the election without additional

documentation or procedures such as signing an affidavit, the poll book reports this and guides the poll worker through the process of obtaining the necessary documentation, affidavits, and signatures. If the voter is not in the correct polling place, the poll worker can instantly generate directions to the correct polling place and give them to the voter either on paper or by sending them to the voter's mobile device.

vi. If the voter is required to sign the poll book in order to receive a ballot, the voter's signature is captured using the poll book's touchscreen. Regardless of whether a signature is required, the poll worker either affirms to the poll book that a ballot has been distributed or cancels the operation and does not distribute a ballot (cancellation can take place at any point in the above procedure).

b. If a voter requires a provisional ballot, the procedure is as follows:
    i. A poll worker enters the relevant voter information (name, address, identification information, etc.) into the poll book.
    ii. The voter's signature is captured using the poll book's touchscreen.
    iii. The poll book uses the provided information to automatically determine the appropriate polling place (if applicable to provisional voting). It displays this information, as in step (a. iv.) above, and the interaction with the system continues from that point with the addition of a notation within the system that the ballot is being cast provisionally. At this point, the voter is registered system-wide as needing to cast a provisional ballot, so if they go to a different polling place (or return to the same polling place), they can be looked up and their information does not need to be re-entered from scratch; this also prevents voters from obtaining multiple provisional ballots.
c. At the opening (closing) of the polls at each polling place, a poll worker must tell one of the poll books at that polling place that the polls are opening (closing). This is done using a simple user interface, with authentication similar to that described in (4) above. Nothing more is required of poll workers, since the peer-to-peer poll book system keeps all election data synchronized and consistent across all the poll books in the entire system; when all polling places have closed, the system as a whole reports that the election is complete. At this point, election reports can be generated (using any poll book) and, assuming that live updating of the CVRS was not being performed during the election, the necessary data can be exported to update the CVRS.
d. The system has a "Google simple" user interface with clearly defined operations, minimal choices to be made by poll workers at any step, and online help available for every function. In the unlikely event that technical support is required, poll workers can use a live Internet chat-based interface to work directly with support personnel during the election, in addition to more traditional telephone-based technical support.

7. The system's reporting is completely flexible; it stores all logs and data in databases on which arbitrary queries can be executed. The system can generate any type of report

desired by the client, and these can be arbitrarily customized.

The system can be audited by examining its tamper-evident, cryptographically secure logs. The same level of customization applies to audit reports as to regular data reports. In addition, at the closing of the polls, the system provides reconciliation information that allows election officials to check the actual numbers of used ballots of all types and styles against the expected numbers of ballots based on polling place check-ins of those types recorded by the electronic poll books.

8. Implementation of this system would be carried out over a period of 9–12 months. This would include the software construction (7–8 months), customization for Rhode Island's specific set of requirements (1 month), verification and validation (concurrent with construction, plus up to 1 additional month), acceptance testing (1–2 months), training (1 week), and system delivery.
9. We do not anticipate that software maintenance or upgrades will be required. If any defect is discovered in the software at any time after delivery, regardless of whether an extended support agreement is in effect, we will fix the defect and deliver updated software at no cost.

   Any required modifications to the software as a result of election law changes or minor State requirement changes after delivery are included for the duration of our contract with the State, and also as part of any extended support agreement; they can be performed at a negotiated one-time cost if no extended support agreement is in place. Hardware maintenance is dependent on the specific COTS systems used to run the software. If the State elects to purchase hardware through us, we can optionally provide hardware support services for the duration of our contract and as part of any extended support agreement.
10. The proposed electronic poll book system is new, and therefore has no history of material defects or failures.

Cost Proposal

The following is a high-level description of our pricing model, and estimated pricing, for the requested electronic poll book system. Should this proceed to the RFP stage, more detail will be provided.

Pricing Model

Galois's primary goal is to increase the trustworthiness and verifiability of all democratic elections worldwide, while also reducing their costs. With that goal, our business model is unlike those of our competitors, so our pricing model is outside the norm.

Our licensing and support model is also unique in the industry and is based upon our technical capabilities and ability to guarantee defect-free products. We offer a permanent

license for a product that you own, with optional annual support contracts for software and hardware. If anyone ever finds a correctness or security flaw in the system, we will fix it for free.

The software license cost is for a license-for-ownership and includes lifetime maintenance, warranty, and support in the form of defect fixes. Our license pricing is based on population and, for our electronic poll book product, is $1.00 per person living in the region served.

The (purely optional) cost of a software support contract (listed below for reference) is fixed and unchanging. That contract includes training, remote and on-site support for your elections, and updates to your software necessitated by changes in law. You are also welcome to contract with any other firm to provide that support, as you will have all the source code and development documentation for the entire system that you own.

Since we exclusively use COTS hardware, our hardware costs are passed straight through to you with no overheads beyond our actual costs of handling (software installation, configuration, etc.). Our cost estimates do not include potential discounts available to you as a large-scale government purchaser, so they are conservative. Moreover, if you have existing hardware compatible with our software system, you can provision and use it in elections. It is also well within your rights and interest, if you wish, to use the COTS hardware purchased for elections for other purposes outside of the election calendar. Complementing our optional software support contract, we are happy to provide a yearly hardware support contract if you wish to purchase one from us.

Finally, while it is likely that the total cost of ownership for your electronic poll book over even a short (e.g., three year) timeframe is likely to be lower with our business model than with our competitors', the fact that our software systems have an effectively arbitrarily long shelf life (because they are guaranteed bug-free and run on whatever platform you decide) means that your per-election costs for electronic poll books effectively trend to zero in the long term.

Estimated Pricing

The following table shows our estimated pricing for the requested electronic poll book system. We have assumed that you will want to provide printers in the polling places (separate from any existing ballot-on-demand printers) to print directions and election information for voters upon request. We have also assumed that you will provide Internet services for the electronic poll books using LTE wireless hotspot devices through a national cellular carriers. The costs incurred as a result of these assumptions are indicated in the table ("Bluetooth/Wireless Printer", "Printer Ink", "Internet Hotspot Devices", and "LTE Data Usage").

As previously mentioned, our cost estimates do not include potential discounts on hardware, consumables, and cellular service available to you as a large-scale government purchaser. Also recall that our maintenance contracts are optional; our one-time perpetual software license fee includes lifetime maintenance, warranty, and support of the delivered software in the form of defect fixes.

Item	Cost
Software	
Development, Testing, and Deployment	$700,000
Perpetual License (described above)	$1,100,000 (based on population)
Annual Maintenance (optional)	$250,000 per year
Hardware **(459 locations, 1200 poll book units,** **500 of other per-location hardware devices)**	
Electronic Poll Book Unit	$500 x 1,200 = $600,000
Bluetooth/Wireless Printer	$250 x 500 = $125,000
Internet Hotspot Devices	$200 x 500 = $100,000
Annual Maintenance (optional)	$40,000 per year
Per-Election Costs	
LTE Data Usage	$30 x 500 = $15,000
Printer Ink	$10 x 500 = $5,000
Totals	
One-time Costs	$2,625,000
Optional Support Costs	$290,000 per year
Per-Election Consumables Costs	$20,000 per election