Galois portions of South Carolina response

DO NOT EDIT
DOCUMENT HAS BEEN EXPORTED

Joe Kiniry <kiniry@galois.com>
23 November 2015

Outline

- About Galois
  - legal name and address
  - point of contact
  - references available
  - letter of introduction
    - elections, high-assurance, security, expertise with certification, work with EAC+NIST and other governments, past experience in elections' security
- Elections R&D
  - open source, component-based, open standards-based, high-assurance, COTS software and hardware, multi-platform
- Elections Products
  - EPB, BMD, ballot delivery, RBMD, tabulation, transitive audits and RLAs, PQM, VVM, other frameworks and capabilities (e.g., logging, protocols, security)
- Elections Services
  - tabulation, various forms of audits, instruction/training
- Implementation Approach
  - rigorous software engineering, work closely with client with full transparency, modular approach for phased certification and rollout of products and services
- Support, Staffing, Help Desk Services
  - how it works, how it is different than most companies operate, field support vs. remote support, service level agreements
- Typical Contract Formulation
  - contractual guarantees about correctness and security, milestone-based deliverables, working with VARs and local integrators
  - example contract outline
- Pricing
  - perpetual licenses and ownership with transparent per-citizen costs, fixed cost development work, plain pricing on services, direct pass-through on COTS costs, COTS configuration and delivery costs, optional hardware and software yearly support costs, flexible payment schemes
- Final Recommendation

- Galois spin-out today and local/SC integrators and support in the future

About Galois

Legal name and address

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

References

Available on request from both federal and industrial clients.

Letter of introduction

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 over 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 sixteen-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, also called a 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. Our technical focus is on creating election systems that are publicly owned open source technology on COTS hardware. Our business focus is on continuously decreasing the per-vote cost of elections henceforth.

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 several prototype products in this space that include an electronic poll book, a verifiable in-person voting system, and tabulation and auditing systems that support multiple voting methods, including ranked choice voting. We are in the process of spinning out a class B corporation whose mission is to bring open source, high-assurance, end-to-end verifiable elections to the world.[1] 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 the class B spinout, 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

[1] The name of this spinout class B corporation is being finalized now.

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.[2]

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[3]) and has supervised numerous BSc, MSc, and PhD theses focusing on elections technologies.[4] 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 an active member of the NIST-EAC Public Working Groups.[5]

Dr. Zimmerman, the Technology Lead at the elections spinout, 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.[6] 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 the Secretary of State of Ohio.

Margaret MacAlpine, Auditing Specialist at the elections spinout, has managed risk limiting and transitive audits in Florida, Connecticut, and most recently in Colorado. She has served as

[2] See https://www.verifiedvoting.org/
[3] See http://www.demtech.dk/
[4] See http://www.kindsoftware.com/
[5] See http://www.nist.gov/itl/vote/nist-voting-public-working-groups.cfm
[6] See https://en.wikipedia.org/wiki/Hursti_Hack

an advisor to 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.[7]

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.

Summary of Products and Services Offered

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, remote ballot delivery and marking, 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 normal plurality elections (e.g., first-past-the-post) and rank choice voting.

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 mandatory 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.

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

[7] See https://estoniaevoting.org/findings/paper/

architecture features an air gap between the software responsible for running an 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,[8] 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.

To witness correctness, 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, we achieve quality assurance through strict configuration management and systematic validation of the code as well as all the evidence-based artifacts and documentation we produce.

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-

[8] See http://cryptol.net/

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 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.[9] Our process, method, tools and technologies span several deployment and development platforms, specification and programming languages, and communication and coordination schemes. Consequently, we produce high-assurance software running on everything from commodity operating systems, such as Microsoft Windows and Apple's OS X, mobile operating systems, such as Google's Android and Apple's iOS, and more esoteric operating environment, such a real-time operating systems, embedded architectures, and even operating system-less services in the cloud called unikernels.

Elections Products

Our software solutions are 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). For prototyping such products we use 3D printing and laser cutting technology.

In general, our systems are designed such that they have sufficient redundancy that no separate disaster recovery environment is required.

Beyond computational requirements, we provide guidelines for how to purchase and install systems in order to maximize security. Testing is built into the software, and does 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 a client.

[9] See https://en.wikipedia.org/wiki/Design_by_contract and https://en.wikipedia.org/wiki/Formal_verification

Elections Services

Our services include:

1. **demonstration**: formal demonstrations of products, particularly tabulation and various forms of auditing
2. **execution**: formally conduct a tabulation or audit in concert with elections officials
3. **engagement**: provide services to help engage the public in elections
4. **analytics**: perform various kinds of useful analytics on elections artifacts
5. **archival**: scan, securely archive, or publicly disclose ballot images
6. **anonymization**: ensure that a set of marked ballot images includes no inappropriate information that may violate voter privacy
7. **education**: teach a course in how to conduct a tabulation, a transitive audit, or a risk-limiting audit

We provide these services either by visiting an elections office (**local**) or via a webcast (**remote**). The latter involves less overhead and cost.

We provide these services with an aim to teach LEOs the tools of the trade so that they can operate independently, and at costs that are geared toward not being overly fiscally burdensome and have a low margin.

Implementation Approach

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, it must be preceded by extensive user and system testing in a production simulation environment like a model office or a mock election.

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.

In general, we recommend that clients have milestones for conducting mock elections in 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) and jurisdictions (small to large) 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.

Support, Staffing, 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.

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 and our perpetual licensing model is meant to drive the cost per-vote of client's elections down with each and every election.

Pricing

Contracts at Galois are either fixed-term, fixed-price contracts or are service contracts that have a simple and transparent per-unit pricing scheme. Development contracts, unless they involve unusual research aspects, are usually fixed-price contracts. Services are usually per-unit priced.

Galois provides a pass-through cost for COTS hardware and consumables, thus imposes no overhead on such costs. If a client requests that COTS systems are purchased, configured, shipped, or maintained by Galois, then there are simple and transparent costs for such.

Development Pricing

To develop a bespoke system for a client, Galois typically modifies an open source implementation specific to that client's needs. The cost of that development is borne by the client via a fixed-price contract whose value is directly proportional to the effort necessary to perform the customization. Given that nearly all of Galois's developers have PhDs in Computer Science, our development effort levels and timelines are typically much shorter than any other organization.

Product Pricing

Products are sold to clients via perpetual licenses. Once a client purchases a system from Galois they own that system, including all of its development artifacts such as specifications, source code, etc., to do with as they will. This ownership is concretized via a perpetual license for those artifacts. The cost of these licenses is based upon (a) the product being licensed, and (b) the total population of the licensing entity.

All licensed products are customized by Galois for the licensee to:

A. conform to all local laws, ordinances, regulations, and rules;
B. fit into the local electoral process and infrastructure (both technical and procedural); and
C. have a polished user-experience tuned for the customer (e.g., customer-defined logos, typefaces, color scheme, etc.).

Galois supports its products perpetually. If a licensee ever discovers a defect in a Galois product, it is immediately fixed for free.

Software License Contracts and Pricing

Perpetual licenses are priced according to simple and transparent metrics. Each product has a per-citizen—or in the case of the polling queue monitor, per-polling place—cost. Thus, if a client knows their population, then they know the approximate cost of a license. The following table includes our current per-citizen costs for our full range of products.

Product	**$/citizen**	**Example cost to South Carolina for a perpetual software license**
Electronic Poll Book	$1	$4,900,000 (approx.)
Remote Ballot Delivery	$1	$4,900,000
Remote Ballot Marking	$1	$4,900,000
Ballot Marking Device	$3	$14,700,000
Verifiable Vote-by-Mail	$1	$4,900,000
Electronic Voting System[10]	$5	$24,500,000
Tabulation System	$1	$4,900,000
Auditing System	$1	$4,900,000
Polling Queue Monitor	$100/ polling place	$250,000
Bundled price for all products	$10	$49,000,000

Our one-time perpetual software license fee includes lifetime maintenance, warranty, and support of the delivered software in the form of defect fixes. Payment terms for licensing fees are flexible, especially for clients that intend to use our systems indefinitely.

Maintenance Contracts and Pricing

Maintenance contracts are completely optional. Galois also offers a yearly software support and maintenance contract. If a client has such a contract, if there are small changes to local law, ordinances, regulations, or rules that require small changes to the product, Galois implements those changes. If the client needs questions answered about the product that are not included in the product's operational materials (its Developers Guide, User's Guide, website, FAQ, etc.), then we answer those questions for free.

[10] Note that the Galois Electronic Voting System includes an electronic pollbook, a ballot marking device, a tabulation system, and an auditing system.

Finally, Galois also offers a yearly hardware support contract. If a client has such a contract, we correct any issues with hardware immediately or replace the hardware.

The base cost of a yearly software support and maintenance contract is 10% of the cost of the perpetual license.

The base cost of a yearly hardware support and maintenance contract is 5% of the cost of the hardware.

Services Pricing

Our current services costs are summarized in the following tables. Below the tables are the principles underlying these services. The costs of some example contracts are found in the following section.

On-Site Services	
All On-Site Services	Base cost of $6,000 per day plus travel and materials
On-Site Tabulation or Audit Demonstration	$1/ballot (tabulation) $10/ballot (audit)[11]
Official On-Site Tabulation or Audit	$2/ballot (tabulation) $20/ballot (audit)[12]
Full Day Course	flat rate of the base cost of $6,000 above; supporting a maximum of 20 participants

The total number of days to conduct any tabulation or audit service is based primarily upon the time spent scanning ballots. Tabulating or auditing an election requires scanning all ballots. The rate of ballot scanning on a commodity scanner for a proficient operator using an automatic paper jogger is approximately 2,000 ballots per hour. A single operator can use one jogger and three scanners concurrently, and therefore scan between 5,000 and 6,000 ballots per hour.

Off-Site Services	
All Off-Site Services	Base cost of $3,000 per day
Off-Site Tabulation or Audit Demonstration	flat rate of the base cost of $3,000 per day; supporting a maximum of 20 participants

[11] Cost is capped at 2x the base cost per day. Thus, if a tight election mandates auditing more than 300 ballots, all additional ballots that are audited in that 8 hour day are audited for free.

[12] Cost is capped at 2x the base cost per day. Thus, if a tight election mandates auditing more than 300 ballots, all additional ballots that are audited in that 8 hour day are audited for free.

Full Day Course	flat rate of the base cost of $3,000 per day; supporting a maximum of 20 participants

Principles for Services

Several foundational principles are the bedrock of our service offerings:

- Providing off-site official tabulation or audits is inappropriate.
- Providing both tabulation and auditing services using the same technology is inappropriate.
- Election artifacts should never leave the control of election authorities without their express permission, and data storage and transport of those artifacts must be accomplished in a third-party verifiably secure fashion.

Typical Contract Formulation

A typical Galois contract for a bespoke software system includes development costs, a perpetual license cost, optional annual software and hardware maintenance, COTS hardware and consumables costs, and training costs. Several example cost breakdowns follow.

For these examples, we will show a cost analysis over a decade time frame, as history has shown us that is about how long traditional vendors' systems will operate.

We strongly recommend potential clients obtain fully rolled-up quotes from existing vendors for a ten year contract so that cost comparisons can be made. Note that you need not request a new quote from us, as our pricing is transparent and requires no internal discussion on our part.

We also recommend reflecting upon the fact that, with our contracts, clients own their products, can hire anyone they like to extend, evolve, and support them, and, because they are high-assurance and open source, the public will have higher confidence in the outcome of every election.

Certification Costs

The costs included in these contracts do not include the cost of obtaining state or federal certification of the products.

Galois has extensive experience in facilitating federal certification of cryptographic systems, thus we understand well how to operate in such an environment and how to optimize development and internal validation and verification to expedite, and thereby tremendously decrease the cost of, certification. Our main differentiator in the certification game is the third party verifiable evidence that we produce as part-and-parcel of our rigorous engineering methodology.

Example 1: Electronic Poll Book

For example, let's presume that a medium-sized jurisdiction with 1,000,000 citizens wants a bespoke open source electronic poll book developed for them, a variant of the Galois Digital Voting List system. They wish to purchase a perpetual license and yearly software support, but will be purchasing and configuring their own COTS hardware with guidance from Galois and obtaining hardware maintenance from a local vendor.

The cost of the development, testing, and deployment is very much dependent upon how unique the client requirements are. If those requirements are quite close to the baseline features of the open source system we have developed, it takes less effort to customize the system for the client. If the client has very unusual or extensive requirements, the effort level will be larger, and thus more costly. In either case, this component of the contract is fixed price.

For this particular example, let's presume that the requirements are moderate, and only about one man-year of labor is necessary to perform the development, testing, and deployment of the system.

Contract component	**Cost**
Electronic Poll Book perpetual license	$1,000,000
One-time, fixed-cost development costs	$500,000
Yearly software maintenance costs	$100,000/yr
Total cost over 10 years	**$2,500,000**

Example 2: Central Count Tabulators

In this example a medium-sized county with 1,000,000 voters wishes to purchase a perpetual license for the Galois Tabulation system for use in a central count setting. The county is using a traditional plurality voting method and only wants a bit of customization on the user interface of the tabulator, so the development costs are low and the timeline is short. The county wishes to have a local IT firm support the Tabulator software.

To tabulate all ballots within a two day timeframe, the county opts for purchasing ten high speed scanners. The county asks Galois to purchase and configure those ten scanners and a tabulation server, and provide hardware maintenance. Finally, the county wants Galois to provide a one day course on tabulation every year for all new officials.

Contract component	**Cost**
Tabulator perpetual license	$1,000,000

One-time, fixed-cost development cost	$100,000
Tabulation server	$5,000
Ten high-speed scanners	$250,000
Hardware maintenance support	$12,750/yr
One day tabulation course	$5,000/yr
Total cost over 10 years	**$1,532,500**

Example 3: Full Voting System

In this example a medium-sized state with a population of 5,000,000 wishes to purchase a perpetual license for the Galois Electronic Voting System. The state uses a traditional plurality voting method and only wants a moderate amount of customization on the user interface and integration with their existing Election Management System. The state wishes to have local firms support both the software and the hardware of the system, leveraging the expertise of some of their current local vendors who understand open source systems.

Contract component	**Cost**
Electronic Voting System perpetual license	$25,000,000
One-time, fixed-cost development cost	$1,000,000
COTS hardware components cost	$5,000,000
Total cost over 10 years	**$31,000,000**

Note that, in those instances where a client chooses to have a local firm perform software or hardware maintenance, the fully burdened cost of the use of the system over a ten year timeframe is incomplete. It is our expectation that, as we have seen in the cost of support contracts for other open source products (such as Linux, cloud web services, etc.), such costs will be significantly less than we see with traditional proprietary IT firms.

Comparison to Existing Vendors' Contracts and Cost

It is important to reflect upon the value of a perpetual license on COTS hardware when comparing costs between two vendors. As an example, consider the long-term cost of a traditional vendors' electronic voting system in a medium-sized state.

In that scenario:

- the state does not own the product;
- the state negotiates an enormous set of fixed-term licenses for the solution from another vendor, including licenses for the product, hardware, firmware, software, etc.; and
- the state effectively cannot have any other vendor compete to maintain either the software or the hardware of the product due to its proprietary nature.

The cost of a contract with Galois is comparable to the cost of a contract with a competing vendor over a single election cycle timeframe.[13] However, in the medium-to-long term, Galois's offering is much less expensive. Moreover, with Galois, the client owns the system, has a perpetual support contract, and has a rigorously engineered system that is contractually guaranteed to operate correctly and securely on inexpensive COTS devices forever.

The Future of Elections

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 our high-assurance, open source elections technologies, much as we have witnessed over the past two decades for Linux and other major open source platforms.

Final Recommendations

[13] We assume a four year pay period for the initial Galois contract, to make "apples-to-apples" comparisons with what traditional vendors offer. Galois offers several payment models.