# DQ Cover Sheet: Attachment D

| | |
|---|---|
| **Company Name** | Galois DBA Free & Fair |
| **Address** | 421 SW 6th Ave., Suite 300 |
| **City/State/Zip** | Portland, OR 97204-1622 |
| **Phone/Fax** | 971-808-3247/503-350-0933 |
| **Email Address** | contact@freeandfair.us |
| **Signature** |  |
| **Typed/Printed Name** | Joseph Kiniry |
| **Title** | CEO & Chief Scientist |
| **Date** | 17 May 2017 |

# Pricing Sheet: Attachment B

| Item | Price |
|---|---|
| **Total Cost for the Risk-Limiting Audit system** (per above specifications) | $99,190 |

| Activity/Task | Price |
|---|---|
| **Detailed Project Plan** | $22,325 |
| **Acceptance of final iteration of code or system after UAT by CDOS** | $22,325 |
| **Offeror's notice that code or system is ready for release in production environment** | $22,325 |
| **Final acceptance of code or system by CDOS after successful use in 2017 Coordinated Election** | $22,325 |
| **Platform/Infrastructure Price (2 units, see attached quote for per-unit price)** | $9,690 |
| **Total Price** | $99,190 |

# Vendor Response Sheet: Attachment C

## Tell us about your experience developing software applications relevant to the scope of work and requirements described in this solicitation (a web-based application requiring populating, querying and reporting on data in a relational database)?

We will first summarize our organization. Then we will provide a summary of the expertise of our key performers on this project for Colorado.

### Free & Fair

Free & Fair's mission is to bring open source, high-assurance, end-to-end verifiable elections to the world. In this response, Free & Fair[1] proposes to create an open source Risk-Limiting Audit tool for the State of Colorado. This system will fulfill the technical requirements stipulated in DQ # VAAA 2017-1420, and will leverage as much existing technology (commercial or open source) as possible.

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

- world-class expertise in high assurance open source election systems and risk-limiting audits,
- an unparalleled record delivering high assurance tools and systems to the most demanding clients in the USA on time and within budget,
- vast experience with creating, contributing to, and managing Open Source Software, and a deep knowledge of Open Source licenses and business cases, and
- corporate principles that focus on transparency, security, and affordability.

We reflect upon these points in the following pages of this summary of our company.

#### World-class Expertise

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

- Free & Fair has, in aggregate, nearly 100 years of open source experience spanning over 100 open source projects, including experience resolving the security issues raised by use of commercial off-the-shelf (COTS) hardware.

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

- Free & Fair staff have been involved with, or are the originators of, some of the most influential, high-profile open source projects in the world. The breadth of our contributions is remarkable, and includes the world's most popular operating system (Linux, Android phones and many other consumer electronics devices), libraries for secure communication and storage (e.g,. SSL libraries and cryptography on many recent LG smartphones), programming languages (e.g., Java, Fortran, and Eiffel), programmer tools (e.g., Emacs, Eclipse, and numerous plugins to modern IDEs), compilers (e.g., the GNU compiler toolchain and the clang/LLVM toolchain), graphics (e.g., Mesa, the library which provides 3D rendering on many platforms), and a plethora of tools used for teaching about and building high assurance systems (OpenJML, ESC/Java2, EBON, Cryptol, SAW, and more).

- Our CEO and Chief Scientist, Dr. Joseph Kiniry, is widely known in the election integrity and scientific communities for his fifteen years of work pursuing a vision of high assurance election systems for trustworthy democracy.

Another strength is our ability to attract and manage excellent subcontractors. We commonly work with world-class firms, small and large, as well as top universities in achieving our ambitious research, development, and engineering goals.

### On Time and Within Budget

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

Free & Fair is already deeply familiar with election technology and risk-limiting audits. One of the seven election technology demonstrators we have developed, called OpenRLA, implements a risk-limiting audit system similar in fundamentals (but not in deployment properties) to the system we propose here. Based on our experience with these demonstrators, we expect to develop a system for Colorado quickly. We have used our election technology prototypes to enhance our understanding of the state-of-the-art and to demonstrate the style and quality of our software development capabilities. While OpenRLA fulfills some of Colorado's requirements implicit in this DQ, it was not designed for high assurance, nor for use in large-scale production environments. Thus, OpenRLA itself will not be part of the proposed system. However, our experience gained while developing it will speed our development of the proposed system.

### Open Source Veterans

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

- All software we have developed and that we propose to develop is open source, which allows inspection by any person interested in assuring or improving the security or functions of the voting system.

- All hardware proposed is Commercial off-the-shelf (COTS).

### Security for "Critical Infrastructure"

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

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

We propose to build election technology for Colorado that meets the highest standards for software design and security, such as those stipulated by the U.S. National Institute of Standards and Technology (NIST) and similar agencies in Canada. The software development techniques specified by NIST have proven effective for building software without bugs. While these techniques may be new to the election community, key members of the Free & Fair project team have used them for 17 years in government contracts totalling over $160M. We have developed products for governments and secured those products against persistent threats from nation-state actors (such as Russia or North Korea) and insider attacks. Free & Fair proposes not merely to fulfill the Colorado requirements, but to fulfill the requirements with systems as secure as the other systems already designated "critical infrastructure" by DHS.

NIST Special Publication 800-160[2] specifies *high-assurance systems*, also known as trustworthy systems. These systems are designed from first principles to be free of flaws. These include flaws related to system correctness, security, reliability, assurance, and more. High-assurance systems are used in situations where failure can lead to loss of life (e.g., an automated train) or have enormous financial implications (e.g., digital cash in smart cards).

Free & Fair project team members have successfully developed many high assurance systems that face many of the same challenges (correctness, security, usability, accessibility, etc.) and use the same technologies (operating systems, programming languages, distributed systems, cryptography, etc.) required by election systems. Our development process and methodology—cited prominently in NIST Interagency Report 8151,[3] written for the White House—includes strict adherence to design, code, and documentation standards, provides easily verifiable evidence for implementation correctness and security, and incorporates the writing and generation of comprehensive test suites for every component of the system. Free &

[2] NIST Special Publication 800-160: *Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, https://doi.org/10.6028/NIST.SP.800-160
[3] NIST Interagency Report 8151: *Dramatically Reducing Software Vulnerabilities,* https://doi.org/10.6028/NIST.IR.8151

Fair will bring the high assurance of safety and mission-critical systems to the election systems and services market, at low cost, and with publicly owned open source technology on COTS hardware.

### Deployment Track Record

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

- **High Assurance Cyber Military Systems (HACMS):** Tools to generate provably secure code for vehicles. Used by Boeing to “hack-proof” the unmanned Little Bird.
- **CyberChaff:** Advanced network defense system that leverages distraction and obfuscation. Deployed by a Fortune 50 company and at universities.
- **Copilot:** Software to detect and report critical hardware failures before they cause accidents. Funded and deployed at NASA.
- **Cryptol:** Toolset to create and verify encryption software. Funded by NSA and deployed across US government.
- **Software Analysis Workbench (SAW):** Toolset to help scientists and engineers formally verify computer programs and establish provable correctness and security guarantees. Deployed by Amazon to provably guarantee the correctness of encryption software.

### Other Statements Material to this RFP

Nothing in this DQ response is proprietary or secret. Free & Fair publishes all of its RFI and RFP responses for government agencies, all proposals we write for Foundations and research funding agencies, and all artifacts relevant to our open source, rigorously engineered, high assurance election systems. As such, unless Colorado wishes otherwise, we will publish this response in the coming weeks.

## Project Members

**Dr. Joseph Kiniry** is Chief Scientist and CEO of Free & Fair. Prior to working for Free & Fair, Dr. Kiniry provided commercial and public consultancy services to several governments on matters relating to elections, their technology, security, processes, and verifiability. He has worked on election systems for fifteen years; has audited the security, correctness, and reliability of numerous physical and Internet-based voting systems; and has developed

high-assurance prototypes and products of several election technologies (including, but not limited to, tallying, auditing, voting, ballot marking, and e-poll book (EPB) systems).

Dr. Kiniry has formally advised four national governments (the USA, The Netherlands, the Republic of Ireland, and Denmark) on matters relating to digital elections and has testified before two parliaments. He has also provided informal input and advice to the governments of Norway, Estonia, and the United States. He co-founded and co-ran a multi-year research project on digital elections (the DemTech project[4]) and has supervised numerous B.S., M.S., and Ph.D. theses focusing on election technologies. His research group developed several high-assurance peer-reviewed election software systems, including a tally system used in binding European elections for The Netherlands in 2004 and an EPB system used in Danish national elections in 2012. Dr. Kiniry has served as a Principal Investigator on research projects for the European Union Council, various Department of Defense branches, the National Science Foundation, and several national funding agencies in Ireland, The Netherlands, and Denmark. He has also started and run a half dozen technology firms and has held tenured positions at four university in three countries. He holds five advanced degrees, including a Ph.D. from the California Institute of Technology.

**Joe Ranweiler** is a software engineering consultant for Free & Fair. He has over 5 years of professional experience building software, spanning research and development, data engineering, and commercially-deployed web applications. Joe helped write Free & Fair's end-to-end verifiable voting system demonstrator, including its core cryptographic components. He is a regular open-source software contributor and was recently the technical lead on Free & Fair's OpenRLA risk-limiting audit system prototype, which was built using modern web application technologies. Joe has a B.S. in Mathematics from Arizona State University.

**Neal McBurnett** has been developing open source software related to election audits for over a decade, and worked as a software developer for tools and the Internet as a Distinguished Member of Technical Staff at Bell Labs for two decades before that. He consulted with the Colorado Secretary of State on the Colorado Risk-Limiting Audit project, and is a member of the team that worked with County Clerk Dana DeBeauvoir in Travis County, TX on the design and RFP for STAR-Vote, a novel voting system supporting end-to-end and risk-limiting audits. He served as vice-chair of the IEEE P1622 standards committee on a common data format for elections, and continues to participate in the U.S. Election Assistance Commission's VVSG-Interoperability Working Group, developing standards for Cast Vote Records and related formats. Using his open source web-based ElectionAudits software, Boulder County, CO performed nationally-recognized audits in 2008 and 2010. He also audited the groundbreaking open source Scantegrity end-to-end election in Takoma Park, MD in 2011. Mr. McBurnett was a major contributor to "Principles and Best Practices for Post-Election Audits" (September 2008) and the 2010 American Statistical Association statement on Risk-Limiting Small Batch Audits. He has participated actively in election processes since 2002 as an observer, election official,

[4] http://demtech.dk/

auditor and public witness. He is an active participant in the Election Verification Network. He holds an M.S. in Computer Science from the University of California at Berkeley, and a B.S. in Computer Science from Brown University.

**Dr. Daniel Zimmerman**, the Technology Lead at Free & Fair, has extensive experience in formal methods, high-assurance software engineering, concurrent and distributed systems, and foundations of computer science. He taught computer science at multiple universities for over a decade. In industry, he has worked primarily in the areas of rigorous software engineering and verifiable election technology. He holds three advanced degrees, including a Ph.D., all from the California Institute of Technology.

**Dr. Joey Dodds** has focused mainly on research and development facilitating correctness proofs for a variety of programs, including cryptographic algorithms. At Free & Fair, Dodds has implemented both a tabulator and a risk-limiting audit system and written formal specifications for both. He also fully proved the correctness of the tabulator. He is a key participant in the verification of Amazon's s2n library, responsible for both the verification of the library and implementing a system to automatically report metrics about the progress of the project to Amazon's upper management. He holds a Ph.D. from Princeton University and holds two other advanced degrees.

**Dr. Stephanie Singer** has developed web-based applications querying relational databases to make customized reports of election results available to the general public. As a member of the Philadelphia County Board of Elections in Pennsylvania, she oversaw the creation and deployment of a modern voter-facing election website. She also held a tenured position in mathematics at Haverford College for over a decade and earned several degrees, including a Ph.D. in mathematics from NYU.

**Mike Kiniry** is a communication expert, with backgrounds in radio, print, and photojournalism, who specializes in clearly communicating complicated concepts. He spent nearly a decade as a public radio reporter, producer, and host and has been a freelance writer and photographer for the past 15 years. Mike is also a videographer and editor, and is the Election Verification Network's dedicated videographer/media producer.

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

# Describe how you will address this project, including staff, time needed, and how you will conform to the timeline set for this project?

The time-to-delivery of this project is extremely short, so it is critical that we take an efficient, economical approach to building the proposed RLA software tool. We view the RLA tool specified in this DQ as a reimplementation and extension of our existing, open source RLA product demonstrator, OpenRLA. The Free & Fair team has extensive pre-existing RLA software development experience and deep domain knowledge. This experience, together with a grounding in lightweight formal methods for high-assurance software engineering, will enable us to build a secure, user-friendly RLA application within the limited timeline.

it is our expectation that the contract start date will be in the week of June 19, 2017. Any delay may affect performer availability and create significant risk of the project not succeeding.

## Project Management Practices

In this section we review Free & Fair's project management practices, which we have used to deliver millions of dollars worth of high assurance systems on time and under budget. Our core project management principles focus on **Customer Caretaking**, **Social Contracts**, **Continuous Improvement**, **Artifacts and Evidence**, and **Transparency**.

### Customer Caretaking

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

### Social Contracts

Our systems engineering artifacts capture technical interdependencies between project team members, but the glue that holds the team together and makes the team work well is our collective social contracts. Our performers explicitly discuss and acknowledge client-supplier relationships between team members and always perform to exceed not only the expectations of our external client (in this case, the Colorado Department of State), but also each internal client (another team member).

### Continuous Improvement

Social contracts are renegotiated frequently and fluidly and are directly reflected upon immediately upon completion. For example, at the end of a thirty minute stand-up meeting discussing a milestone that we just reached and what comes next, we often have a five minute

discussion about what worked well and where improvements can be made with regards to that particular piece of work. In particular, we focus on its embedded social contracts. The individuals in our organization always attempt to maximize efficiency, impact, and joy at work.

### Artifacts and Evidence

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

### Transparency

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

## Project Management Structure and Responsibilities

Dr. J. Kiniry holds final responsibility for the success of this project. Dr. Zimmerman and Dr. Dodds, working with Dr. J. Kiniry, will write the system specification, design and verify the client/server communication protocol and the server/server synchronization protocol, and implement the server-side and communication subsystems, including the audit computation subsystem and the datastore subsystem. Ms. Miller will work with Mr. Ranweiler and Mr. McBurnett on the UX of the system and will mock up UIs. Mr. Ranweiler is responsible for designing and implementing the client side of the system against the system specification and the UI/UX design. Mr. McBurnett will provide domain expertise in Colorado elections and ballot-level comparison risk-limiting audits, will red team system architecture, design, and implementation, and will perform Q/A on the tool, and will help write documentation. He will also coordinate with the EVN CORLA2 team to get statistical algorithm input, advice, and feedback, and will be on call during deployment for the trial runs of the tool during Logic and Accuracy testing and after the election until the audits are done. Mr. M. Kiniry will write the user guide for the system and will revise the developer’s documentation. Dr. Singer will be the customer caretaker and project lead.

## Technical Aspects

To fulfill Colorado's requirements, we will use a modular system design and standard, well-understood web application technologies. We propose a Java-based web application running on a Linux server, hosted in the CDOS data center. We *strongly* recommend using a JVM version that supports Java 8 (which is supported by WebSphere 9.0), but our proposal is *not* contingent on this. We propose a standard SQL relational database management system (the specific deployment choice to be negotiated during contracting) for data persistence. As the user interface (UI) will be browser-based, we propose writing the client in TypeScript, a mainstream, Microsoft-supported variant of JavaScript that offers opt-in, Java-like type safety. TypeScript compiles to plain, human-readable JavaScript, so this choice will support client-side correctness without requiring any special web browser support. If Colorado insists upon using raw JavaScript, we will accommodate.

We summarize first the behavioral properties, and then the critical non-behavioral properties, of the system we will develop for Colorado.

### Behavioral properties summary

This new tool for Colorado, which we will call OpenRLA for the remainder of this proposal, will guide users through all the steps defined in the DQ.

Ballot manifests and cast vote records (CVRs) will be uploaded to the server via HTTPS.

The status of uploaded data will be summarized in a state-wide dashboard, along with information on which counties have not yet uploaded their CVRs, and uploads that have formatting or content issues. The status of data, and results as audits are performed, will be provided for each contest to be audited.

Random selections of ballots for performing a ballot-level comparison risk limiting audit will be automatically generated based on the provided random seed using the SHA-256-based pseudo-random number generator specified in the DQ, as well as the computed contest margins and other indicated parameters including any discrepancies found.

A county view of the audit will display information on the progress of each audited contest in the county, with a summary of discrepancies.

We will tailor view/edit permissions for each screen of information to users with appropriate authorizations as defined by the state.

Public access to appropriate data and reports will be provided in standard file formats.

### Non-behavioral properties summary

We summarize our approaches to three critical non-behavioral properties of OpenRLA below: how we achieve fault tolerance, how we perform synchronization, and some reflections on the dynamism of the UI and user experience (UX).

### Fault tolerance

We have built many fault tolerant distributed systems over the years. For example, Dr. Kiniry was co-architect of Sprint's Internet Service Provider product (what later became a part of Earthlink) in 1995. While the underlying platforms and technology have evolved several times since then, the underlying principles remain the same.

For this particular application, we propose a two server deployment, preferably in separate locations which have independent power subsystems and network backbones. Each server will have two power supplies and two network cards, which should be on separate, independent subnets. Servers will have hot-swappable SSDs in a RAID 5 configuration for local data redundancy and fault tolerance.

### Synchronization

We can design a distributed synchronization protocol in either a primary/secondary architecture (with support for dynamic failover in the case of network or system unavailability) or in a peer-to-peer configuration, where inbound requests can go to either server using DNS load balancing. We can also use a distributed synchronization mechanism already integrated into the client-selected backend database system, if that is an appropriate choice. The decision of what synchronization protocol to use will be made in consultation with the client.

### UI and UX Dynamism

Rather than simply create a plain-old-HTML front-end, our UI and UX will use rich JavaScript UI libraries to create a browser-based user experience that feels like a modern application one might find in any of the mainstream online app stores. Our UX expert will work with the client to ensure that the UI's dynamism and presentation facilitates OpenRLA's critical users, election officials running audits.

## Timeline & Staffing

Note: this timeline is contingent on a Contract Start Date no later than Monday, 6/19/2017.

| **Time period** | **Staffing Level (approx. aggregate FTE)** | **Deliverable** |
|---|---|---|
| 6/19 through 7/14 | 4.75 FTE (3 engineers, 0.5 customer caretaker, 0.5 documentation writer, 0.75 UX expert) | initial code or system to CDOS, with run books, installation guides & user manuals |
| 7/31 through 8/4 | 1.5 FTE (1.25 engineers, 0.25 customer caretaker) | second iteration of code or system that fixes bugs and deficiencies identified by CDOS |
| 8/14 through 8/18 | 2 FTE (1.25 engineers, 0.25 documentation writer, 0.25 customer caretaker, 0.25 UX) | final iteration of code or system to CDOS |
| 8/28 through 9/8 | 0.5 FTE (0.25 engineers, 0.25 customer caretaker) | support load and penetration testing |

# Describe how your proposed solution will conform to the CDOS security requirements stated in the specification sheet.

We will build our solution to be hosted in CDOS data centers. In this proposal, we will therefore only explicitly address issues not implicitly addressed by this choice. Concretely, due to planned hosting in CDOS data centers, all of the following items are implicitly addressed:

- System fault-tolerance, redundant hosting, and fail-over
- GeoIP blocking, IP whitelisting/blacklisting
- Web application firewalling
- Web application penetration testing and vulnerability scanning
- Distributed denial-of-service prevention
- Anti-malware scanning and other host protections, such as file and configuration integrity monitoring
- Centralized logging
- Network segmentation
- Systems administration and remote access

We now address the remaining security requirements.

### User management and controls

Upon user registration, users will be prompted to create a password conforming to the requirements listed in [CO-RLA-DQ, 13]. For authentication and authorization we will either integrate with the existing CDOS User Management System or implement the following best practices.

- Passwords will be salted and stretched using a secure key-derivation function such as PBKDF2 or Argon2, which can be tuned to increase the work factor required for password guess attempts.
- Two-factor authentication will be provided via the Time-Based One-Time Password (TOTP) algorithm or another two-factor scheme negotiated with the client.
- Policies around password expiry, access attempt controls, and session duration limits will be enforced by the application in accordance with [CO-RLA-DQ, 13] or more recent NIST standards, as negotiated with the client.
- User provisioning and password management will be performed by Free & Fair, coordinated with the state.

### System operations, security, and privacy

Free & Fair engineers are experts in secure software engineering practices, and regular clients include the Department of Defense and the United States intelligence community. All software will undergo a documented security review before production release, and will be specifically audited against the OWASP Top 10. In particular, the RLA application will satisfy the Colorado State OIT Secure Applications Coding Standard as described in [TS-CISO-006].

### Systems hardening and protection

Free & Fair-delivered systems will be hardened according to best practices. Any sensitive data, including personally-identifiable information (PII), will be stored encrypted. Application-level logging will be implemented using syslog and standard Java logging mechanisms, which will then be aggregated by CDOS-provided centralized logging, using NTP for time synchronization. We will build the system with the security design principles we have used for years for Department of Defense and U.S. intelligence community clients.

## Please describe to us your business continuity plan, including your redundancy, hosting and fail over backup plan.

We propose hosting in the CDOS data center, which will support failover, as described in the Documented Quote [CO-RLA-DQ, p. 16]. Our quote includes all necessary features for fault tolerance summarized earlier, including a redundant standby server with separate network cards and power supplies, dual CPUs, and hard drives in a RAID 5 configuration. We expect regular backups to be configured to use CDOS Disaster Recovery facility.

As for business continuity, we will apply techniques we have been developing since the 1990s to create systems for clients requiring no more than 0.001% downtime. These techniques include practical applied formal methods (the application of mathematical techniques to the design, development, and assurance of software systems) and a peer-reviewed rigorous systems engineering methodology.[5] Our methodology was recently recommended by a NIST internal report (IR 8151 "Dramatically Reducing Software Vulnerabilities"), presented to the White House Office of Science and Technology at their request in November, 2016.[6]

## Please include 2 references from government projects: (State, higher education, political subdivisions, counties, etc.)

1. Name of organization/agency: US Department of Labor
Name of contact: Tambra Leonard
Phone number: (202) 693-5744
Email: leonard.tambra@dol.gov
Brief 1-2 sentence description of finished project: Free & Fair principals performed a quality and security audit of an Internet Voting system used by most unions in the USA, and also provided expert input into national policy in union elections.

2. Name of organization/agency: National Institute of Standards and Technology (NIST)
Name of contact: Paul Black
Phone number: 301-975-4794
Email: paul.black@nist.gov
Brief 1-2 sentence description of finished project: Free & Fair principals created formal verification technology for the National Institute of Standards and Technology (NIST). This technology focuses on verifying properties of modern C code, which uses new keywords to enable developers to specify the use of novel memory models for modern multi-core systems.

- Have all requirements for this solicitation, as stated above, been met? **Yes**
- Do you accept Colorado Contract Terms and conditions? **No**
- If No is marked to the question above, have you included a statement of explanation to the contract terms and conditions as an additional attachment? **Yes, see below**
- Have you included your vendor W-9? **Yes**
- Have you included a copy of your Insurance policy? **Yes**

[5] See "A Verification-centric Software Development Process for Java" (http://ieeexplore.ieee.org/abstract/document/5381513/?reload=true) and "Secret Ninja Formal Methods" (http://link.springer.com/chapter/10.1007/978-3-540-68237-0_16), both of which are authored by Dr. Kiniry and Dr. Zimmerman.
[6] See NIST IR 8151 (http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8151.pdf)

## Statement of Explanation to the Contract Terms and Conditions

We stipulate that Colorado's RLA tool should be developed in an open, transparent fashion (e.g., in a public GitHub repository—we suggest our existing OpenRLA repository or a fork thereof) and must be made available to the public under an Open Source Initiative (OSI) approved open source license.[7] We suggest either or both of the BSD and GPLv3 licenses, per our current license policy at Free & Fair.[8]

We urge the Colorado Department of State to ensure that the contract start date will be during the week of June 19, 2017. Any delay may affect performer availability and create significant risk of the project not succeeding.

[7] See the Open Source Initiative website at https://opensource.org

[8] See our article, "Open Source and Elections" at http://freeandfair.us/articles/open-source/ and our LICENSE text for the OpenRLA repository at https://github.com/FreeAndFair/OpenRLA/blob/master/LICENSE

# Current Vendor W-9

Galois, Inc's current W-9 appears on the next page. Note that Galois, Inc., does business as Free & Fair.

Form **W-9**
(Rev. December 2014)
Department of the Treasury
Internal Revenue Service

# Request for Taxpayer Identification Number and Certification

**Give Form to the requester. Do not send to the IRS.**

Print or type
See Specific Instructions on page 2.

1 Name (as shown on your income tax return). Name is required on this line; do not leave this line blank.
**Galois, Inc.**

2 Business name/disregarded entity name, if different from above

3 Check appropriate box for federal tax classification; check only **one** of the following seven boxes:
☐ Individual/sole proprietor or single-member LLC ☑ C Corporation ☐ S Corporation ☐ Partnership ☐ Trust/estate
☐ Limited liability company. Enter the tax classification (C=C corporation, S=S corporation, P=partnership) ▶ _____
**Note.** For a single-member LLC that is disregarded, do not check LLC; check the appropriate box in the line above for the tax classification of the single-member owner.
☐ Other (see instructions) ▶

4 Exemptions (codes apply only to certain entities, not individuals; see instructions on page 3):
Exempt payee code (if any) _____
Exemption from FATCA reporting code (if any) _____
*(Applies to accounts maintained outside the U.S.)*

5 Address (number, street, and apt. or suite no.)
**421 SW Sixth Avenue, Suite 300**

Requester's name and address (optional)

6 City, state, and ZIP code
**Portland, OR 97204**

7 List account number(s) here (optional)

## Part I Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. The TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the Part I instructions on page 3. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN* on page 3.

**Note.** If the account is in more than one name, see the instructions for line 1 and the chart on page 4 for guidelines on whose number to enter.

**Social security number**
[ ][ ][ ] – [ ][ ] – [ ][ ][ ][ ]

**or**

**Employer identification number**
9 3 – 1 2 7 8 5 4 0

## Part II Certification

Under penalties of perjury, I certify that:

1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
2. I am not subject to backup withholding because: (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
3. I am a U.S. citizen or other U.S. person (defined below); and
4. The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.

**Certification instructions.** You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions on page 3.

**Sign Here** Signature of U.S. person ▶ David L Boyer Date ▶ 5/24/17

## General Instructions

Section references are to the Internal Revenue Code unless otherwise noted.

**Future developments.** Information about developments affecting Form W-9 (such as legislation enacted after we release it) is at *www.irs.gov/fw9*.

### Purpose of Form

An individual or entity (Form W-9 requester) who is required to file an information return with the IRS must obtain your correct taxpayer identification number (TIN) which may be your social security number (SSN), individual taxpayer identification number (ITIN), adoption taxpayer identification number (ATIN), or employer identification number (EIN), to report on an information return the amount paid to you, or other amount reportable on an information return. Examples of information returns include, but are not limited to, the following:

- Form 1099-INT (interest earned or paid)
- Form 1099-DIV (dividends, including those from stocks or mutual funds)
- Form 1099-MISC (various types of income, prizes, awards, or gross proceeds)
- Form 1099-B (stock or mutual fund sales and certain other transactions by brokers)
- Form 1099-S (proceeds from real estate transactions)
- Form 1099-K (merchant card and third party network transactions)
- Form 1098 (home mortgage interest), 1098-E (student loan interest), 1098-T (tuition)
- Form 1099-C (canceled debt)
- Form 1099-A (acquisition or abandonment of secured property)

Use Form W-9 only if you are a U.S. person (including a resident alien), to provide your correct TIN.

*If you do not return Form W-9 to the requester with a TIN, you might be subject to backup withholding.* See *What is backup withholding?* on page 2.

By signing the filled-out form, you:

1. Certify that the TIN you are giving is correct (or you are waiting for a number to be issued),
2. Certify that you are not subject to backup withholding, or
3. Claim exemption from backup withholding if you are a U.S. exempt payee. If applicable, you are also certifying that as a U.S. person, your allocable share of any partnership income from a U.S. trade or business is not subject to the withholding tax on foreign partners' share of effectively connected income, and
4. Certify that FATCA code(s) entered on this form (if any) indicating that you are exempt from the FATCA reporting, is correct. See *What is FATCA reporting?* on page 2 for further information.

# Dell Quote for Hardware

A quote for Dell hardware is included on the following pages. Note that we require two of the units that are priced here at $4844.73 each, for a total of $9689.46.

# A quote for your consideration!

Based on your business needs, we put the following quote together to help with your purchase decision. Please review your quote details below, then contact your sales rep when you're ready to place your order.

**Total:$4,844.73**

| **Quote number:** | **Quote date:** | **Quote expiration:** | **Solution ID:** |
|---|---|---|---|
| 3000014037257.1 | May 23, 2017 | Jun. 22, 2017 | 8162903 |

| **Company name:** | **Customer number:** | **Phone:** |
|---|---|---|
| GALOIS, INC | 95388433 | (503) 626-6616 |

**Sales rep information:**
Kyle Kinser
Kyle_Kinser@Dell.com
(800) 456-3355
Ext: 5133432

**Bill to:**
GALOIS, INC
421 SW 6TH AVE
STE 300
PORTLAND
OR 97204
US
(503) 626-6616

## Pricing Summary

| Item | Qty | Unit price | Subtotal |
|---|---|---|---|
| PowerEdge R430 - [dellstar_11598] | 1 | $4,844.73 | $4,844.73 |

DBC as low as $146.00 / month^

| | |
|---|---|
| **Subtotal:** | $4,844.73 |
| **Shipping:** | $0.00 |
| **Environmental Fees:** | $0.00 |
| **Non-Taxable Amount:** | $4,844.73 |
| **Taxable Amount:** | $0.00 |
| **Estimated Tax:** | $0.00 |
| **Total:** | **$4,844.73** |

## Lease Products*

| Months | Finance Lease | Fair Market Value (FMV) |
|---|---|---|
| 60 | $107.43 | NA |
| 48 | $128.09 | $129.20 |
| 36 | $168.12 | $148.36 |
| 24 | $245.35 | $206.49 |
| 12 | $450.78 | $392.38 |

Special lease pricing may be available for qualified customers. Please contact your DFS Sales Representative for details.

# Dear Customer,

Your Quote is detailed below; please review the quote for product and information accuracy. If you find errors or desire certain changes please contact me as soon as possible.
Regards,
Kyle Kinser
Order this quote easily online through your Premier page,
or if you do not have Premier, using Quote to Order

## Shipping Group 1

**Shipping Contact:**
PENI NORTHCOTT

**Shipping phone:**
(503) 626-6616

**Shipping via:**
Standard Ground

**Shipping Address:**
421 SW 6TH AVE
STE 300
PORTLAND
OR 97204
US

| SKU | Description | Qty | Unit Price | Subtotal |
|---|---|---|---|---|
| | **PowerEdge R430 - [dellstar_11598]** | **1** | **$4,844.73** | **$4,844.73** |
| 210-ADLO | PowerEdge R430 Server | 1 | - | - |
| 384-BBMW | PowerEdge R430/R530 Motherboard MLK | 1 | - | - |
| 461-AADZ | No Trusted Platform Module | 1 | - | - |
| 321-BBNK | 2.5" Chassis with up to 8 Hot Plug Hard Drives | 1 | - | - |
| 340-AMJF | PowerEdge R430 Shipping | 1 | - | - |
| 338-BFFU | Intel Xeon E5-2630 v3 2.4GHz,20M Cache,8.00GT/s QPI,Turbo,HT,8C/16T (85W) Max Mem 1866MHz | 1 | - | - |
| 374-BBHD | Intel Xeon E5-2630 v3 2.4GHz,20M Cache,8.00GT/s QPI,Turbo,HT,8C/16T (85W) Max Mem 1866MHz | 1 | - | - |
| 370-ABXP | DIMM Blanks for System with 2 Processors | 1 | - | - |
| 370-ABXV | Cooling Fan | 1 | - | - |
| 374-BBIJ | 135W Heatsink | 1 | - | - |
| 374-BBIJ | 135W Heatsink | 1 | - | - |
| 370-ACPH | 2400MT/s RDIMMs | 1 | - | - |
| 330-BBEF | Riser with Two x16 PCIe Gen3 LP slots (x16 PCIe lanes), R430 | 1 | - | - |
| 370-AAIP | Performance Optimized | 1 | - | - |
| 780-BBPN | RAID 5 for H330/H730/H730P (3-8 HDDs or SSDs) | 1 | - | - |
| 405-AAEG | PERC H730 Integrated RAID Controller, 1GB Cache | 1 | - | - |
| 385-BBIK | iDRAC8, Express | 1 | - | - |
| 429-AAQM | DVD ROM SATA Internal | 1 | - | - |
| 770-BBBL | ReadyRails Sliding Rails With Cable Management Arm | 1 | - | - |

| | | | | |
|---|---|---|---|---|
| 325-BCJU | Dell EMC 1U Standard Bezel | 1 | - | - |
| 384-BBBL | Performance BIOS Settings | 1 | - | - |
| 450-AEGZ | Dual, Hot-plug, Redundant Power Supply (1+1), 550W | 1 | - | - |
| 631-AACK | No Systems Documentation, No OpenManage DVD Kit | 1 | - | - |
| 619-ABVR | No Operating System | 1 | - | - |
| 421-5736 | No Media Required | 1 | - | - |
| 332-1286 | US Order | 1 | - | - |
| 989-3439 | Thank you choosing Dell ProSupport. For tech support, visit http://www.dell.com/support or call 1-800- 945-3355 | 1 | - | - |
| 997-2924 | Dell Hardware Limited Warranty Plus On Site Service | 1 | - | - |
| 997-2934 | ProSupport: Next Business Day Onsite Service After Problem Diagnosis,4 Year | 1 | - | - |
| 997-2949 | ProSupport: 7x24 HW / SW Tech Support and Assistance, 4 Year | 1 | - | - |
| 900-9997 | On-Site Installation Declined | 1 | - | - |
| 909-0259 | Dell Proactive Systems Management - Declined - www.dell.com/Proactive | 1 | - | - |
| 973-2426 | Declined Remote Consulting Service | 1 | - | - |
| 370-ACNQ | 8GB RDIMM, 2400MT/s, Single Rank, x8 Data Width | 4 | - | - |
| 400-AMID | 480GB Solid State Drive SATA Mix Use MLC 6Gbps 2.5in Hot-plug Drive, SM863 | 3 | - | - |
| 542-BBCO | On-Board LOM 1GBE (Dual Port for Towers, Quad Port for Racks) | 2 | - | - |
| 450-AALV | NEMA 5-15P to C13 Wall Plug, 125 Volt, 15 AMP, 10 Feet (3m), Power Cord, North America | 2 | - | - |

| | |
|---|---|
| **Subtotal:** | $4,844.73 |
| **Shipping:** | $0.00 |
| **Environmental Fees:** | $0.00 |
| **Estimated Tax:** | $0.00 |
| **Total:** | **$4,844.73** |

# Important Notes

## Terms of Sale

Unless you have a separate written agreement that specifically applies to this order, your order will be subject to and governed by the following agreements, each of which are incorporated herein by reference and available in hardcopy from Dell at your request: Dell's Terms of Sale (www.dell.com/learn/us/en/uscorp1/terms-of-sale), which include a binding consumer arbitration provision and incorporate Dell's U.S. Return Policy (www.dell.com/returnpolicy) and Warranty (for Consumer warranties; for Commercial warranties).

If this purchase includes services: in addition to the foregoing applicable terms, the terms of your service contract will apply (Consumer; Commercial). If this purchase includes software: in addition to the foregoing applicable terms, your use of the software is subject to the license terms accompanying the software, and in the absence of such terms, then use of the Dell-branded application software is subject to the Dell End User License Agreement - Type A (www.dell.com/AEULA) and use of the Dell-branded system software is subject to the Dell End User License Agreement - Type S (www.dell.com/SEULA).

You acknowledge having read and agree to be bound by the foregoing applicable terms in their entirety. Any terms and conditions set forth in your purchase order or any other correspondence that are in addition to, inconsistent or in conflict with, the foregoing applicable online terms will be of no force or effect unless specifically agreed to in a writing signed by Dell that expressly references such terms.

## Pricing, Taxes, and Additional Information

All product, pricing, and other information is valid for U.S. customers and U.S. addresses only, and is based on the latest information available and may be subject to change. Dell reserves the right to cancel quotes and orders arising from pricing or other errors. Please indicate any tax-exempt status on your PO, and fax your exemption certificate, including your Customer Number, to the Dell Tax Department at 800-433-9023. Please ensure that your tax-exemption certificate reflects the correct Dell entity name: **Dell Marketing L.P.**
Note: All tax quoted above is an estimate; final taxes will be listed on the invoice.

**If you have any questions regarding tax please send an e-mail to Tax_Department@dell.com.**

For certain products shipped to end-users in California, a State Environmental Fee will be applied to your invoice. Dell encourages customers to dispose of electronic equipment properly.

**^Dell Business Credit (DBC):**

OFFER VARIES BY CREDITWORTHINESS AS DETERMINED BY LENDER. Offered by WebBank to Small and Medium Business customers with approved credit. Taxes, shipping and other charges are extra and vary. Minimum monthly payments are the greater of $15 or 3% of account balance. Dell Business Credit is not offered to government or public entities, or business entities located and organized outside of the United States.

***Dell Financial Services Lease:**

1. This proposal is property of Dell Financial Services and contains confidential information. This proposal shall not be duplicated or disclosed in whole or part. Minimum transaction size $500.
2. All terms are subject to credit approval, execution and return of mutually acceptable lease documentation.
3. Lease rates are based upon the final amount, configuration and specification of the supplied equipment. Interim rent may apply and be due in the first payment cycle.
4. The Lease Quote is exclusive of shipping costs, maintenance fees, filing fees, licensing fees, property or use taxes, insurance premiums and similar items, which shall be for Lessee's account.
5. This proposal is valid through the expiration date shown above, or, if none is specified, for 30 calendar days from date of presentation.

# Vendor Exhibit A:
# Hourly rates for additional vendor work

| | |
|---|---|
| Engineer | **$100** |
| Senior Engineer | **$125** |
| Documentation | **$75** |
| Customer Care | **$180** |
| UI/UX | **$80** |

# Copy of our current insurance policy

Galois, Inc.'s current liability insurance and umbrella liability insurance policy declarations are included on the following pages. Note that Galois, Inc. does business as Free & Fair.

CHUBB®

# Liability Insurance

## Declarations

**Chubb Group of Insurance Companies**
**15 Mountain View Road**
**Warren, NJ 07059**

*Named Insured and Mailing Address*

GALOIS INC.
421 SW 6TH AVE. STE 300
PORTLAND, OR 97204

*Policy Number* 3584-78-86 WCE

*Effective Date* MAY 17, 2017

*Issued by the stock insurance company indicated below, herein called the company.*

**FEDERAL INSURANCE COMPANY**

*Producer No.* 0070912-99999

*Incorporated under the laws of* INDIANA

*Producer* HUGGINS INSURANCE SERVICES INC
1786 STATE STREET
SALEM, OR 97308-0000

## Policy Period

From: MAY 17, 2017 To: MAY 17, 2018
12:01 A.M. standard time at the Named Insured's mailing address shown above.

| Liability Coverage | Limit Of Insurance |
|---|---|
| *GENERAL LIABILITY* | |
| GENERAL AGGREGATE LIMIT | $ 2,000,000 |
| PRODUCTS/COMPLETED OPERATIONS AGGREGATE LIMIT | $ 2,000,000 |
| EACH OCCURRENCE LIMIT | $ 1,000,000 |
| ADVERTISING INJURY AND PERSONAL INJURY AGGREGATE LIMIT | $ 1,000,000 |
| DAMAGE TO PREMISES RENTED TO YOU LIMIT | $ 1,000,000 |
| MEDICAL EXPENSES LIMIT | $ 10,000 |

CHUBB®

| **Liability Coverage** *(continued)* | **Limit Of Insurance** | |
|---|---|---|
| *EMPLOYEE BENEFITS ERRORS OR OMISSIONS* | | |
| AGGREGATE LIMIT | $ 1,000,000 | |
| EACH CLAIM LIMIT | $ 1,000,000 | |
| DEDUCTIBLE - EACH CLAIM | | $ 1,000 |
| RETROACTIVE DATE | | MAY 17, 2007 |
| *STOP GAP - OHIO* | | |
| AGGREGATE LIMIT | $ 500,000 | |
| BODILY INJURY BY ACCIDENT - EACH ACCIDENT LIMIT | $ 500,000 | |
| BODILY INJURY BY DISEASE - EACH EMPLOYEE LIMIT | $ 500,000 | |
| DESIGNATED STATE | | OHIO |

Chubb. Insured.℠

CHUBB®

# Chubb Commercial Excess And Umbrella Insurance

## Declarations

**Chubb Group of Insurance Companies**
**15 Mountain View Road**
**Warren, NJ 07059**

*Named Insured and Mailing Address*

GALOIS INC.
421 SW 6TH AVE. STE 300
PORTLAND, OR 97204

*Policy Number* 9364-01-86

*Issued by the stock insurance company indicated below, herein called the company.*

**FEDERAL INSURANCE COMPANY**

*Incorporated under the laws of* Indiana

*Producer No.* 0070912-99999

*Producer* HUGGINS INSURANCE SERVICES INC
1786 STATE STREET
SALEM, OR 97308-0000

### Policy Period

From: MAY 17, 2017 To: MAY 17, 2018
12:01 A.M. standard time at the Named Insured's mailing address shown above.

### Premium

$ 5,250.00

### Limits Of Insurance

| | | |
|---|---|---|
| Excess Coverage Other Aggregate Limit (as applicable) | $ | 4,000,000. |
| Umbrella Coverages Aggregate Limit | $ | 4,000,000. |
| Products Completed Operations Aggregate Limit | $ | 4,000,000. |
| Advertising Injury and Personal Injury Aggregate Limit | $ | 4,000,000. |
| Each Occurrence Limit | $ | 4,000,000. |

### Authorization

In Witness Whereof, the company issuing this policy has caused this policy to be signed by its authorized officers, but this policy shall not be valid unless also signed by a duly authorized representative of the company.

**FEDERAL INSURANCE COMPANY**

*Secretary* *President*

*Authorized Representative*

*February 27, 2017*

Chubb. Insured.℠