FREE & FAIR

Response to Elections Canada RFI for Voting Services Modernization / Polling Place Process Enhancement

RFI/RFP #	ECRS-RFI-16-0167a
RFI/RFP Subject	Voting Services Modernization / Polling Place Process Enhancement
Proposer's Name	Galois, Inc., DBA Free & Fair
Type of Organization	Other Small Business
Technical Point of Contact	Dr. Joseph Kiniry 421 SW Sixth Avenue, Suite 300 Portland, OR 97204 503.808.7228, kiniry@freeandfair.us
Administrative Point of Contact	Jodee LeRoux 421 SW Sixth Avenue, Suite 300 Portland, OR 97204 ph 503.808.7209, contracts@galois.com
Date Proposal Prepared	April 28, 2017
Closing Date of RFI/RFP	Apri 28, 2017

Executive Summary

Free & Fair is pleased to respond to **ECRS-RFI-16-0167A: Voting Services Modernization / Polling Place Process Enhancement**. Our RFI response summarizes our firm, some of our past relevant work, and our development and service offerings that are relevant to this RFI.

The systems we propose to create are open source, high assurance, and publicly owned. We propose many innovative ideas to support Elections Canada's goals.

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] makes a number of suggestions for the upcoming RFP and proposes to create an innovative, open source, high assurance, publicly owned electronic poll book system for Elections Canada. This system will fulfill the technical requirements stipulated in Elections Canada's future RFP, and will leverage as much existing technology (commercial or open source) as possible.

Free & Fair is exactly the right entity to realize Election Canada's vision because we have:
- world-class expertise in high assurance open source elections systems;
- an unparalleled record in 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 Executive Summary.

Our world-class expertise is concretized in three main dimensions relevant to Elections Canada:
- Free & Fair has, in aggregate, nearly 100 years of open source experience spanning over 100 open source projects, including experience resolving the security issues raised by use of Commercial Off-the-Shelf (COTS) hardware.
- Free & Fair staff members have been involved with, or are the originators of, some of the most influential, high-profile open source projects in the world. The breadth of our work is remarkable, and includes the world's most popular operating system (Linux, used in Android phones and many other consumer electronics devices), libraries for secure communication and storage (e.g,. SSL libraries and cryptography on many recent LG smartphones), programming languages (e.g., Java, Fortran, and Eiffel), programmer tools (e.g., Emacs, Eclipse, and numerous plugins to modern IDEs), compilers (e.g., the GNU compiler toolchain and the clang/LLVM toolchain), graphics (e.g., Mesa, the library that provides 3D rendering on many

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

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 elections integrity and scientific community 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 elections technology. As evidence, we have developed seven product demonstrators, some of which implement much of the functionality of the system we propose here. Based on our experience with these developments, we expect to develop systems for Elections Canada quickly. We have used these prototypes to enhance our understanding of the state-of-the-art in elections technology and to demonstrate the style and quality of our software development capabilities. Two of our existing demonstrators—our electronic poll book ("EPollbook"[2]) and our polling place queue monitor ("Qubie"[3])—fulfills many of Elections Canada's requirements implicit in this RFI. Since these prototypes were not designed for high assurance, nor for use in large-scale production environments, they will not be part of the proposed system. However, our experience developing them will speed our development of the proposed Elections Canada systems.

We expect to cut certification times in half by providing design, code, and validation and verification artifacts immediately to the certifying authority. While we cannot dictate the timelines of independent certification authorities, our development methods produce a comprehensive set of certification artifacts as part of the design and implementation process, so there is no delay between the end of development and the submission of complete materials for certification. An example of this approach is the election tabulation system built by a team led by Dr. Kiniry for use by The Netherlands in the 2004 European Council Elections. This system was developed and certified within 12 calendar weeks instead of the year or more typical for election systems in that country at that time.

---

[2] See http://freeandfair.us/products/epollbook/ for more information about Free & Fair's EPollbook.

[3] See http://freeandfair.us/products/qubie/ for more information about Free & Fair's Qubie.

Open Source Veterans

Traditionally, election technology vendors have profited from limited competition and retaining 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 Elections Canada 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 either COTS or, where custom hardware is required, open hardware, allowing Elections Canada to benefit from open competition among vendors.
- In order to widen Elections Canada's future hardware options, and to encourage a wide community of potential developers and users, all proposed software can be made to run on all mainstream operating systems (Microsoft Windows, Apple OS X, and various Linux flavors).

Security for "Critical Infrastructure"

In preparation for the 2016 U.S. Presidential election, nearly every U.S. state requested help from the U.S. Department of Homeland Security (DHS) to secure election technology. Events such as these requests, and inquiries following the election, have raised public awareness of the importance of security to election administration. Even without a malicious attack, every Election Day brings stories of bugs and glitches that cause a public outcry somewhere, especially if the number of votes affected comes close to a margin of victory. More than ever before, election officials have been asked to assure the public that their elections have been run correctly. 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. elections 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 Elections Canada 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. Most common commercial computing systems depend on "recovery" from occasional crashes (if the screen freezes, just restart it!), but 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 totaling over $160M. We have developed products for governments and secured those products against persistent threats from nation-state actors (such as Russia and North Korea) and

insider attacks. Free & Fair proposes not merely to fulfill the Elections Canada requirements, but to fulfill the requirements with systems as secure as the other systems currently designated "critical infrastructure" by DHS and comparable Canadian agencies.

NIST Special Publication 800-160[4] 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 elections systems. Our development process and methodology—cited prominently in NIST Interagency Report 8151[5], written for the White House—includes strict adherence to design, code, and documentation standards, provides easily verifiable evidence for implementation correctness and security, and incorporates the writing and generation of comprehensive test suites for every component of the system. Free & Fair will bring the high assurance of safety and mission-critical systems to the elections 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.

---

[4] 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

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

- **Cryptol:** Toolset to create and verify encryption software. Funded by NSA and deployed across US government.
- **Software Analysis Workbench:** 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 RFI

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

Conclusion

We are happy to answer any other questions Elections Canada might have about our products and services. We look forward to responding to a future RFP from Elections Canada on this topic.

Responses

No.	Question	Response
1	Based on the information provided regarding Elections Canada's business and technical requirements within specific target development and delivery time frames, are there any areas that may present major challenges, issues or risks? What could Elections Canada do to address these challenges or issues or to mitigate the risks associated with those issues and challenges you may have identified? What should be included in the RFP documents to address those issues and challenges?	We summarize some general challenges, issues, and risks below. We make a number of recommendations for mitigating such and improving the RFP to permit innovation and facilitate risk reduction and fiscal responsibility. 1. If necessary, we will have some of our staff endeavor to obtain appropriate security clearances in Canada. Several of our staff members already have S and TS clearances in the U.S.A. with multiple agencies. We also have performed directly for the CSE on matters relating to national security and cryptography, so we are already have a good relationship with them. 2. There is no explicit mention of accessibility requirements or goals of EC with regards to the Voter Services Modernization / Polling Place Enhancement project. We expect to see significant requirements and goals for such in the RFP. We not only expect to see requirements and features that enable the disabled electors to have a voting experience equivalent to abled electors, but also for disabled citizens to act as returning officers, central poll supervisors, election officers, and the like. We believe that the disabled should be able to be a full-fledged part of all facets of the democratic process. Consequently, our products are developed with usability, accessibility, and security as the three core non-functional feature sets of our products.

No.	Question	Response
1	continued	3. To enable evidenced-based decision making via analytics and business intelligence, one must not only gather relevant and useful data about the electoral process on election day (e.g., a log of all electronic poll book state transitions, as partially specified in this RFI), but one should also gather other static and dynamic information about polling places before and on election day. We have a product called Qubie that does just that in a privacy preserving way, and we intend to propose to integrate Qubie into our EPollbook as a part of our future RFP response. One delicate matter often neglected in this space is elector and officer privacy, as many naive logging or monitoring services do not give evidence that they can or do respect the relevant privacy laws around personally identifiable information. 4. Since universal coverage of adequate cell data is not expected, mandating automatic, low-latency synchronization across EDs or the nation is not reasonable. And one must be careful that national or local law does not mandate inappropriate requirements on synchronization across polling divisions, particularly in the quest to improve elections integrity due to ill-founded fears of voter impersonation fraud, as has been seen in several Canadian and U.S. states over the past several years. 5. In the general, mandating wide-area synchronization across thousands of sites and tens of thousands of systems introduces significant computational, protocol, operational, and deployment complexity. We suggest that a cost/risk analysis is warranted to determine if such synchronization is actually warranted.

No.	Question	Response
1	continued	6. In circumstances where multiple disconnected polling places end up with inconsistent data, the law and operational specifications must be clear about the appropriate resolution. For example, if a voter purportedly votes at more than one advance polling place, there must be clear specifications for how to resolve the data inconsistency after-the-fact, as well as exactly what digital forensic materials must be handed over to the authorities to investigate the possible violation of law. 7. On a related note, mandating a traditional RESTful client-server architecture in the RFP overly constrains innovative firms from offering technical solutions that are perhaps simpler and less costly than such 20th century distributed architectures. We suggest that you specify such an architecture as a model, but not as the definitive architecture, in the RFP to leave the door open for innovation. 8. While informal specification about data and data types and distributed architectural styles are welcome and useful in an RFP, it should be noted that when we mechanically formalize and reason about such specifications we often find numerous errors. The same holds true particularly for workflow diagrams, like those you provide in BPML, and state machine diagrams. Please ensure that the RFP leaves room for the detection and remediation of errors of this nature so that the RFP awardee is not contractually bound to build what is effectively an incorrect system. 9. Likewise, detailed specifications of the means by which security requirements should be fulfilled often limit innovation. For example, insisting upon specific key management schemes or the use of particular older protocols can sometimes lead to a system that is not as secure as it could be. Leave the door open in the RFP for experts in information

No.	Question	Response
1	continued	10. Our standard contract offers support for what you call Corrective and Emergency Maintenance (pg. 44). Our yearly service contract includes what you term Preventative Maintenance, Adaptive Maintenance, and Perfective Maintenance. Recognizing the fact that some organization break down costing of these different maintenance aspects in different ways, leave open the framing of the cost proposal on such to provide flexibility to offerors. E.g., do not insist only upon a time period-based or per-system scheme. 11. There is no mention in this RFI of validation and verification of the protocols, operational behavior, or security of the proposed system. We recommend that a high bar is set for such, given the complexity of the system that is proposed. In particular, designing a distributed synchronization algorithm capable of spanning such a large number of hosts in a partially connected environment is a significant challenge—a challenge we suggest that no existing elections vendor other than ourselves is capable of accomplishing. 12. Finally, we suggest that EC should not overly constrain the financial and use models of the hardware used to run the electronic poll books themselves. Out and out purchasing, storing, and provisioning 60,000 touchscreen devices, relevant networking hardware (both local and wide-area), and their cases for occasional use in local and national elections is perhaps not in the best interest of Canadian taxpayers. Permit innovative organizations to respond to your RFP in a fashion that will fulfill the core requirements and goals of EC and yet avoid such an outlay of tens of millions of dollars in hardware and millions of dollars in operational cost for provisioning, distribution, and more.

No.	Question	Response
1	continued	13. There is an error on page 17, bullet three. Its text and cross-reference are missing.
2	Based on the information provided regarding Elections Canada's business requirements, target development and delivery time frames, is your organization positioned to grow, expand, adjust and form relationships as required to deliver the provisioning and servicing of a solution on a national scale? If not, what could Elections Canada do to address these challenges or issues or to mitigate the risks associated with those issues and challenges you may have identified? What should be included in the RFP documents to address those issues and challenges?	Our organization is growing and expanding as we continue to develop product prototypes, pursue other opportunities, and perform R&D in the space of high assurance elections systems. As discussed in the preface of these answers, we also write and perform on R&D contracts for federal governments and, as we have been winning such contracts at an unprecedented rate, we have been growing to accommodate those clients (primarily the U.S. Department of Defence, Homeland Security, the Intelligence Community, and Fortune 100 companies). As such, this upcoming RFP from Elections Canada represents a significant opportunity for our business, and we will evolve and grow to fulfill EC's goals if we win this contract. Our one recommendation is we suggest that EC describe, but not prescribe, example scenarios of how project management, organizational structure, and support might look in the context of this large project. This will help to ensure that innovative organizations can propose alternative structures, processes, and mechanisms to achieve the same fundamental goals, but in a different fashion and perhaps with less cost and effort. For example, mandating technical personnel to be on-site for extended periods, or the use of particular support technologies or workflows, may not be in EC's best interest as it potentially limits opportunities for innovation.

No.	Question	Response
3	Based on the detailed information provided regarding Elections Canada's Security Requirements: "ISO 27001 certification may constitute a mandatory requirement at the time of RFP response. Do you foresee major challenges, issues or risks?" What could Elections Canada do to address these challenges or issues or to mitigate the risks associated with those issues and challenges you may have identified? What should be included in the RFP documents to address those issues and challenges?	Our organization is not ISO 27001 certified. We are aware of this set of standards, as well as complementary standards from NIST and the IEEE relevant to information systems security. In fact, our parent organization Galois provides consultancy and R&D services relevant to these standards and the technologies to which they apply. If obtaining ISO 27001 certification is a requirement of the eventual RFP, we will endeavor to obtain that certification. We recommend that, if such a certification is mandated, the deadline for obtaining certification should be coupled to a milestone of the project rather than being a precondition on proposal submission. We suggest that by making ISO 27001 or any similar certification a precondition on proposal submission, Elections Canada would be significantly limiting competition and would, in fact, be eliminating virtually all elections technology vendors from consideration. Based upon our experiences with process-centric standards such as ISO 9001 and 27001, we further suggest that Elections Canada should focus less on the box-ticking exercise that this kind of certification represents in the modern age, and more on the results and artifacts produced for Elections Canada. Certification standards like Common Criteria (CC)—about which we provide consultancy services to other firms—while historically more rigorous, time-consuming, and expensive than process standards like those from the ISO, are indicative of excellence in both process and results. While we do not suggest mandatory CC certification of technology, we do suggest that Elections Canada should give objective, evidence-based evaluation of technology significant weight. Our products are designed and developed in a

No.	Question	Response
4	Based on the information provided regarding Elections Canada's business requirements, target development and delivery time frames, particularly with respect to complexity, scale and time criticality, are there factors that Elections Canada does not appear to have considered from your perspective?	The overall timeline for this project is reasonable for a standard IT project developed and deployed by a typical IT consultancy. When 20th century development practices and technologies are used (i.e., agile development practices, hand-written testing, and unsafe languages like C or C++), and when the bulk of developers are not computer scientists, risk mitigation that focuses on early deliveries and a heavyweight oversight process is sometimes necessary. This is particularly true in development situations where systems engineers cannot provide objective evidence about the correctness and security of their system which can be evaluated by arbitrary third parties. On the other hand, companies like Free & Fair perform systems engineering in a fashion that is completely unlike most others. Our development methodology focuses on evidence and assurance of a system's fitness for purpose, correctness, and security. We do provide objective evidence about the correctness and security of our systems which can be evaluated by arbitrary third parties. We do not simply demonstrate correctness by performing time consuming and expensive hand-written testing—testing that only exercises an infinitesimal fraction of the state space of the system—but instead provide mathematical proof that our systems do exactly what we promise—no more, no less. Consequently, the timelines of the projects we run have a decidedly different character. To put it plainly, our project timelines look completely different from the timelines of projects run by a firm like Oracle, IBM, or PWC. As such, we recommend that you state that development timelines provided in the RFP are only indicative, and that concrete timelines for development will be negotiated as a part of the contract with the winning firm.

No.	Question	Response
5	Generally speaking and based on the information provided by Elections Canada in the RFI documentation, do you foresee any barriers, impediments or show-stoppers in responding to this solicitation or for EC to successfully achieve its E-Poll Solution?	The main critique that we have of the RFI is that it too specifically describes the system and its operational model, thereby significantly limiting possible innovation in both systems engineering and deployment. In particular, mandating that up to 60,000 devices must be purchased, housed, provisioned, and deployed is quite possibly an enormous waste of resources. Once again, we suggest that EC write the RFP in such a way that it lays out one possible provisioning and deployment scenario, but leaves open the possibility that innovative firms can submit novel solutions that could save EC, and thus Canadian taxpayers, significant funds.

No.	Question	Response
6	What pricing models are available for, or do you feel would best suit, your solution? - Professional Services – hourly rate by - resource category - Software license fee - Firm lot price per module - Firm lot price per end user - Other, please specify:	Our pricing model is provided in the preface text to this table and is also available on our website. In short, we price a hardened, customized version of our open source technology that runs on COTS hardware on a per-citizen cost basis. The current price of our electronic poll book system is $1 USD per citizen (not per voter). This constitutes a sale, not a time-limited or system-limited license, of a specific version of our system to the client. Thus EC can use and extend this technology into the indefinite future. There is no such thing as “vendor lock-in” with our technology. Our technology becomes your technology in perpetuity. EC can do with the customized software system as they please, perform customization or extension of the system themselves, or use any other contractor that they wish for the system. In fact, we recommend that clients use their existing IT support services and consultants with whom they already have quality relationships for such services. Moreover, we offer to purchase and provide hardware at cost, and provide a fixed cost contract for system testing, provisioning, and deployment. Finally, we offer yearly support contracts for both software and hardware support with transparent pricing. The current price of such an SLA is 10% of the system cost per year for software support and 5% of the hardware cost per year for hardware support.