



## LECTIO REFORMO™

By **E. John Sebes & Gregory A. Miller**  
© 2007 Open Source Digital Voting Foundation

### AN ABBREVIATED AMERICAN E-VOTING MANIFESTO<sup>1</sup>

#### INTRODUCTION

The deplorable state of U.S. voting technology and its adoption has motivated this Manifesto. We've been thinking about this paper for a long time. This paper is what we've learned and believe. And it is time to act. The U.S. Tech Sector has a history of tackling difficult problems head-on. It's our hope that this paper and the efforts of OSDV will rally the collective creativity, ingenuity, and effort of all corners of the U.S. Tech Sector – from the Silicon Valley to the Research Triangle, to the 128 Loop, to the Silicon Forest, and everywhere. We hope you agree and join us in this important effort.

Publicly elected government is a cornerstone of Democracy. The greatest threat to the vitality of Democracy is lack of trust in the process of voting and election results. For elections to retain any real meaning, confidence must be maintained in this country's system of conducting elections in a reliable transparent manner. The system must accurately capture the will of each voter and the electorate as a whole. A 21<sup>st</sup> century democracy should find significant value in the adoption of technology in the process of voting. Technology should be a trustworthy asset to Democracy; however, so far, the opposite appears to be the case.

In fact, the fastest growing problem with U.S. elections today is *digital voting*. Americans found a way past the “*hanging chad*,” but confidence in the way we vote is now at risk from computerized voting systems that were supposed to be the way forward. Whether its touch screens or electronically counted paper ballots, increasing numbers of precincts are using computers to run elections, and we're seeing more, not fewer problems. Adopting digital voting machines is great for companies that make and sell them, but so far, it's no better for voters. We've witnessed incidents ranging from wrongly recorded votes, to no way to recount, and even security lapses that can open the door to election fraud.

---

<sup>1</sup> This version, also referred to as “*Lectio Reformo Curto*” is a shortened version of our thinking on the importance of the open source digital voting movement, focusing on the problems and the required principles to assure the veracity of digital voting technology and processes. To see the full version of this Manifesto, which provides an important discussion on the principles of open source as applied to the mission of OSDV, please look for “*Lectio Reformo Plenus*” on the Open Source Digital Voting web site at [www.osdv.org](http://www.osdv.org). *Lectio Reformo*, *Lectio Reformo Curto* and *Lectio Reformo Plenus* are trademarks of the Open Source Digital Voting Foundation, a California non-profit public benefit corporation formed pursuant to 501(c)(3) of the U.S. Internal Revenue Code.

And here is another fact: nearly all of these problems lie in basic technical aspects that can be successfully resolved first, before tackling any questions of optimal system design. While the world's Technocrats dream of an ideal system that delivers high assurance voting services any time, any where, the reality on the floors of today's polling places across America are technical train wrecks waiting to happen. Long before building high speed rails, it is essential to ensure the existing trains remain on their tracks. To be sure, we are life-long technologists, however, it is clear to us that no amount of ingenuity applied to creating an ideal voting system will result in anything useful until the veracity of today's digital devices and services is assured and verified – *the outcome being restored confidence and earned trust.*

We submit there are seven (7) principles mandatory to assure the veracity of digital voting. This manifesto articulates those principles. Its worth noting manifestos are often political in nature, and that is *absolutely not* the intention of this paper.

### THE DOUBLE EDGED SWORD OF TECHNOLOGY

It's well settled that computing technology plays an increasing role in how elections are conducted. And it's equally clear that technology has ever-increasing power to strengthen the confidence cornerstone, or undermine it. In the United States, increasing confidence is the theory behind adoption of digital voting technology, while actual experience is the opposite. In this matter of both the public trust at large, and in each citizen's confidence in the reality of their votes, the adage "*perception is reality*" has perhaps its greatest application. From affidavits of individual's voting experience, to demonstrations by technology experts, the basis for distrust is growing, and is magnified by media coverage and public discourse through blogs, e-mail forums, and web sites trained on the issues.

We believe that much of the basis of distrust is rooted in fundamental issues of incorrectly applied technology – issues that can be addressed at the technical level to describe and demonstrate how computing technology can and should be properly applied to digital voting. The tools and techniques are readily available and well-understood, having been applied to a variety of systems. These tools and techniques are "*high assurance computing practices.*" And they can be readily applied to current digital voting technology in a straightforward manner. We believe this approach can allay both doubt and suspicion, and increase confidence in elections conducted with digital voting technology.

### THE 7 PRINCIPLES OF DIGITAL VOTING VERACITY ASSURANCE ("DIVA")

Applying *high assurance computing practices* to voting technology, while straight forward, requires a thorough understanding of principles what we term "digital voting veracity assurance" or "DIVA" for short. We believe these seven principles are condition precedent to declaring any voting technology as having veracity and therefore, trustworthiness:

1. **Comprehension:** The basic mechanics of elections must be easily understandable to the entire electorate, and comprehensible by anyone with an average intelligence commensurate with the age of voting eligibility, including voting, counting, canvassing, re-counting, and creating election results. Therefore, the

complexity of any technology that provides for any of these basic mechanics must be sufficiently abstracted to a point where their operation is comprehensible by this same audience<sup>2</sup>.

2. **Purpose:** Any use of digital voting technology must be solely for the purpose of automating a part of an election system or process that is *already in place* and well-understood in principle.<sup>3</sup>
3. **Specificity:** Any digital voting component must be embodied in a specific device that is defined for a specific purpose in an existing election system.
4. **Compatibility:** Devices must be designed for application that is compatible with existing processes and procedures, without requiring technology-driven changes that can undermine comprehension and confidence.
5. **Assurance:** Devices must be readily assessable for their veracity; this means it performs all (*and only*) its required functions, with a very high degree of integrity and resistance to inadvertent change, or tampering, or fraud.
6. **Certification:** Devices must be able to be easily subjected to an independent certification process void of any vendor advice, direction, influence, instruction, or participation, including meeting assurance assessments by the state or local election officials that procure and operate digital voting technology.
7. **Transparency:** Each certified high-assurance device must be able to be used in a transparent manner of conducting elections, where the processes and results of the election are transparent, auditable, replicable (*for either recount or audit*), and publicly available.

The above 7 principles are simply technology-related extensions to, and in support of, existing rights of voters as participants in elections. The essence of those “*voter rights*” is that the entire voting process should be comprehensible, fair, honest, unbiased, and verifiable, with public access to results and audits.

## TIME IS OF THE ESSENCE

The U.S. (*as in other Democratic nations*) is blessed with an election system that can support these rights, but recent experience has shown that technology can either strengthen or weaken the voting system in its support of these rights. This is becoming a particularly urgent matter given that the upcoming national election – in less than two years – will for the first time since 1953, not offer an incumbent candidate. The two main parties, as well as others who qualify for the ballot, will present new choices for the office of President of the United States.

---

<sup>2</sup> For example, the Apple® Macintosh® employs significant capability (*and technical complexity to do so*), but packages (*read: “abstracts”*) this complexity in such a manner to present the simplest possible interface to the user (*e.g., a one-button mouse and a standard set of menus across all functions*). Likewise, the World Wide Web Browser together with the protocols and services that compose the Web employ significant capability with corresponding underlying complexity, however, for the end user, the use of the web browser is abstracted to simple comprehensible notions of links, pointing, and clicking; going forward and backward, reloading a page, and stopping a page load. Importantly, there is no greater requirement for technical comprehension to use a web browser or a Macintosh.

<sup>3</sup> For example, precinct-level processing of ballots to count votes is a distinct process or part of a system to operate a precinct.

There is no fantasy among us that the challenges of fixing the problems with digital voting, producing high veracity systems, or engineering the ideal system can even remotely be accomplished in that time frame. That said we firmly believe there is significant headway that can be made, and real tools produced to assist the challenges of those who manage and operate voting polls and precincts that can definitely bring about higher assurance in the devices and processes they are charged with employing.

Thus far, digital voting technology has created problems that are more visible than its benefits, thus threatening to significantly undermine confidence. *These problems are urgent* because of increasing occurrences of voting irregularities, increasing media coverage, conflicting information, misinformation, and the potential effect on real elections.

Consider six developments that roughly chronicle the situation to date:

- **Undermined Trust.** Confidence in some states' state and federal elections was significantly eroded in the year 2000 as a result of controversy over apparent arbitrariness of ballot count interpretation, spoiled ballot definitions, difficulty in performing repeatable recounts, etc. In the case of the infamous "*hanging chad*" in Florida, repercussions went to the U.S. Supreme Court, requiring its controversial role in resolving the dispute over the Florida national election results. This ultimately resulted in the Court determining the next President of the United States in a close decision that will likely provide no precedent for future cases due to an unusually narrow application.
- **The Reactionary Fix.** Congress passed the HAVA legislation (*Help America Vote Act of 2002*) leading to the formation of the Election Assistance Commission.<sup>4</sup> We believe this Act, and the charter and purpose of the EAC catalyzed the business opportunity for the widespread adoption of digital voting devices.<sup>5</sup> Accordingly, rapid adoption of digital voting technology ensued over the following years, intended to prevent similar incidents of 2000. This effort led to 2006 elections marred by new side-effects of digital voting including for example, [a] voter attestation of "vote flipping" by digital balloting machines, [b] very close and nationally significant Senate elections in which the margin of victory was far smaller than the number of votes that were unable to be recounted, and [c] controversy over audit capability and the "paper trail."
- **All Eyes Are On It.** Over the past four years, and especially since the mid-term elections of 2006, there has been and continues to be an ever increasing amount of media coverage of these incidents. And there continues to be distortion of the

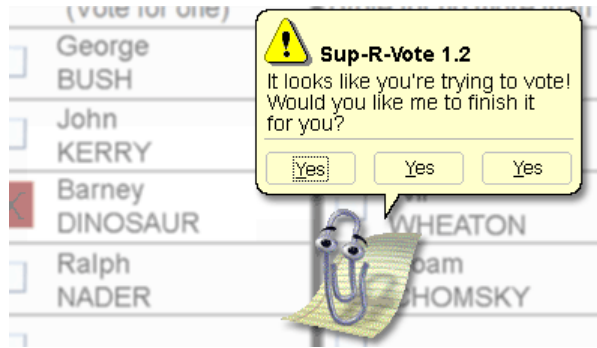
---

<sup>4</sup> See: <http://www.fec.gov/hava/hava.htm>

<sup>5</sup> As explained elsewhere, we further believe that the dynamics and mechanics of the marketplace and business opportunity led to the decision by several vendors to base their digital voting technology on popular computing platforms, which introduced complexities and opportunities for problems discussed in this paper, and which violate the DIVA principles. In fact, this result was predicated on a simple set of business issues including, but not limited to, time-to-market and the required investment (*but lack of acceptable ROI*) in proper R&D to make the kinds of discrete and specific high assurance computing devices necessary for a function of this importance and magnitude – gathering and tallying the votes of Americans. See: *Lectio Reformo Plenus* available at [www.osdv.org](http://www.osdv.org) soon.

facts, circumstances, and situations in public discourse and media, all of which is expedited and magnified through the Internet.<sup>6</sup>

- **The About Face.** In early-2007 Florida announced the decision to abandon millions of dollars worth of digital voting equipment that was used with questionable result in the 2006 “mid-term” elections. This leaves open questions ranging from what Florida will do for 2008, to what comes of the equipment they have and the investment they’ve sunk.
- **Eroding Confidence Continues.** Digital voting technology is becoming the injured Wildebeest pursued by the Media Hyenas. With increasing frequency technical demonstrations are held illuminating the weakness of some types of digital voting equipment, with broad coverage and wide ranging publicity of each event.
- **The “Above the Fold” Issue.** Voting assurance has become a high-profile editorial issue of mainstream media. Now, at this writing, it is on the 110<sup>th</sup> Congressional docket with new legislation being introduced in both the House and Senate. This is making election reform a “political football,” and some say it could become the new “3<sup>rd</sup> rail” of politics.



With this snowballing urgency, digital voting problems are no longer the province of publicity hungry spirited technologists, election gadflies, little-noticed public interest groups, bloggers, and obscure branches of the Federal government. These problems have become the agenda of a wide range of people from humorists, cartoonists, and Hollywood movie-makers, to Presidential candidates, and a mushrooming cadre of public interest and lobbying groups of many kinds. State and local elections officials, as well as Federal government branches like the FEC, EAC, and NIST are seeing previously unimaginable attention on technology issues. But nearly everyone seems consumed with the symptoms and far from captured by the causes.

### EXPOSING THE ROOT CAUSE

Yet for all this exposure, there has been remarkably little attention paid to the root cause and potential solutions – aside from interesting but non-actionable pronouncements of certain types of equipment as being flawed, or calls for fundamental changes to the U.S. election system. While useful fodder for editorials and academic debate (*to say nothing of recent fiction from Hollywood*), these activities have not provided a practical basis for substantial near-term improvement.

In fact, nothing could be further from the truth than assertions that current technology is fundamentally flawed and can only be usefully replaced by a return to purely paper and manual systems. Such a return, implemented with learning from the

<sup>6</sup> It's been said a lie can circle the globe before Truth gets its boots on.

past, might be a viable and simple way to restore confidence. Yet, realistically many state and local election organizations will continue to use digital voting technology, and in fact, it's safe to suggest that over time, the integration (*some say, incursion*) of technology is unstoppable.<sup>7</sup>

For those cases where technology is already an established part of the process, high-confidence digital voting can be achieved by addressing the single root cause of the weakness of current systems, and its two inevitable corollaries.

### The Root Cause

We believe the root cause is the basing of digital voting products on popular, widely available computing systems and software (*familiar to many people in their personal and professional lives*) and then building closed systems on top that are difficult to assess and easy to criticize.

The first corollary is that these systems appear to have unreliable software, that is, voters observe what appear to be software glitches (e.g., *vote flipping, printer problems*) and elections volunteers observe complex systems that are often beyond their ability to operate confidently. For many voters and volunteers, these appearances are unsurprising. After all, they are accustomed to personal computers that are not simple to operate, and which sometimes behave in bewildering ways. While this lack of confidence is commonplace in consumer computing, it's simply unacceptable to building public trust in digital voting.

The second corollary is that voting machines have a basic characteristic that is *wholly undesirable* for special-purpose systems like digital voting equipment: they are easy to access, modify, reconfigure, etc. Yet digital voting equipment must be prepared for a narrow and specific use – “*cast in stone*” – to perform only its exact function during a limited time period (i.e., *before, during, and after Election Day*), and without any alterations within that time frame. However, currently these systems are not – by and large – built that way. So if they are even *potentially* modifiable, it is very difficult to have confidence that a system will stay the same and always function correctly. When apparent glitches or confusion occurs, it is equally difficult to determine whether it's a result of a malfunctioning normal system, or a system malfunctioning because it was modified or prepared erroneously.

Both these corollaries converge in one more effect of the root cause: *A system that can “misbehave” and can also be changed to create new misbehavior is also a system that could have security flaws or vulnerabilities that could be used to create such flaws.*

Although technically enabled (*and potentially widespread and subtle*) election fraud is more a matter of current function or conspiracy theory, the factual basis for this possibility is frequently demonstrated by credible experts, and increasingly given wide currency in the media.

---

<sup>7</sup> According to a study in late 2006 by Election Data Services, Inc., nearly one-third of the nation's registered voters faced new voting equipment in November, compared to the November 2004 election. Since the turbulent presidential election of 2000 and the enactment of the Help America Vote Act (HAVA), jurisdictions with 63% of the nation's registered voters have changed their voting systems introducing some form of technology, marking the largest shift in voting equipment in the nation's history.

Put simply, many people are accustomed to ordinary computers that both seem “flaky” and also have security problems. If digital voting systems are based on computers that are *fundamentally similar*, then it is no wonder than confidence in them is so easy to erode. Most people put up with less than ideal systems for ordinary use because of their benefits: powerful, versatile, able to run an enormous variety of software, and relatively easy to update for enhanced performance or protection. Yet, none of these benefits are required, helpful or appropriate for voting systems – *systems that should be fixed in function and highly critical*. So, it would seem we have an untenable yet intractable situation. **Or do we?**

## RECOGNIZING A ROOT SOLUTION

Ironically, of these defects (*real, apparent, or perceived*) in current voting technology, many are completely unnecessary because of the existence of well-understood means to create functionally similar digital voting devices without any of these “*benefits-turned-flaws*.”

### For the Device (and Makers Thereof)

The overall solution is to build digital voting devices that are *simplified fixed-function systems* rather than complex, powerful, flexible general purpose systems. In technical parlance, these simplified fixed-function systems are *high assurance systems*.

There are actually a modest number of elements to approaching how such devices can be both built as high-assurance systems, and demonstrated to be high-assurance systems. Both are equally important, as “high assurance” consists both of building systems well for specific purpose, and also the ability for others (*besides the builders*) to verify a high degree of assurance, by inspecting systems before choosing to use them.

What should those elements be? Roughly, and at a high level, the following are five principles<sup>8</sup> of design for solutions that will honor the 7 DIVA principles for systems with the limited purpose of polling and voting.

- **Provide Clear Requirements for Capability.** Design each type of device to a clearly stated set of capabilities, and build *only* those capabilities, which will lead to simpler smaller systems that are more feasible to independently assess. Use industry guidelines and applicable standards for defining which types of capabilities to build into the device, *and resist temptation to over-engineer!*
- **Eliminate Ability to Alter Capability.** Ensure that a system, once built, cannot be changed in any way to alter those capabilities or add any other capabilities. For example, there is *never* a justifiable reason under the principles of *Lectio Reformo* to build in “back doors” to a system. Likewise, although good software architecture principles suggest designing for extensibility and reusability, said principles must be restrictively applied to not violate this principle.
- **Eliminate Ability to Modify Data.** Ensure that such a system, when in use, can only create data that is *not* modifiable, *especially ballot data*. In other words, the system should never be able to modify data on its own. To put this in context,

---

<sup>8</sup> This is not intended to be the *Lectio Reformo* comprehensive list of design principles; that remains to be vetted. However, this is the Manifesto core set. From here we intend the Open Source Digital Voting Foundation community to vet a full set of design criteria.

any modification of user (voter) generated data must only be possible by authentication, verification, and validation by the user, and then only through re-tracing the data capture process. For example, under these principles, “*on-the-fly*” corrections would be impossible – that is, a review of a data capture (vote decision) and opportunity to change it there in that context is not allowed. Only [a] re-authentication of the individual, [b] affirmation of an intent to re-process a data capture event (i.e., a specific vote), and [c] a return to the beginning of the process for that specific data capture event (*utilizing the same and standard validation process*) would be allowed.

- **Ensure Capability for Independent Examination.** Provide a means for *feasible, repeatable* independent inspection of such a system to verify the above and other properties. This should not be performed by “black box” testing, but inspection of the “*source code*” building blocks of the system, among other types of examination. Notwithstanding the name of the Foundation – *Open Source Digital Voting (of which we explain the significance and importance of the open source movement elsewhere)*, it is essential to differentiate from a common misconception that this type of inspection requires “*open source software.*” This is simply *not* the case. Open source code is just one way to enable large numbers of people to examine and inspect a system in detail. Despite political rhetoric and agendas of commercial enterprise, it is well settled that a vendor of a system can enable access to a certified and agreed-to independent expert without compromising any intellectual property the vendor has created or owns. A large community of inspectors is not necessary or desirable, nor do we suggest one’s commercial source code, wherein trade secret protection is chosen, be subjected to a public display. However, a discrete process that provides for secured, limited inspection is necessary.
- **Provide a Check & Balance.** Provide for a means to verify that an individual device is exactly the same as another device that was previously assessed for correctness, reliability, and integrity. We believe this concept is simple enough and speaks for itself.

While these principles may seem obvious to many readers, in our opinion, they have been lost on most commercial efforts to date. And this is not because the vendors are incapable of applying these principles, but sadly because a sufficient business case has not yet been made for the limited market<sup>9</sup> of voting devices for polling stations, nationwide.

Nevertheless, we believe that these design principles can be straightforwardly applied to digital voting devices, without undue burden, or any risk of compromising a vendor’s ability to innovate, deliver innovation, and protect advantages of innovation.

---

<sup>9</sup> There are 186,000 polling stations nationwide. Typically a polling station can have from 3 to several dozen voting stations or devices. See: [www.eac.gov/election\\_survey\\_2004/doc/EDS-chap%2013%20poll%20places.doc](http://www.eac.gov/election_survey_2004/doc/EDS-chap%2013%20poll%20places.doc)

In fact, pursuant to “*Lectio Reformo*,” they must.<sup>10</sup>

### For Those Charged With Managing Elections

In a similar vein, we can define guideposts for how state and local elections bodies can specify, evaluate, test, acquire, certify, and use high-assurance digital voting devices, and do so in a way that protects the 7 principles of veracity assurance. At a high level then, we submit these are the top three principles:

- **Define.** Plan on conducting elections with a well-defined process that is specific about the types of digital equipment to be used. Follow industry guidelines and applicable standards for defining which types of equipment to acquire.
- **Assess.** Perform (*or engage services to have performed*) assurance assessments of each candidate product for type of equipment required; or alternatively, re-use a previous assessment made by some other party, and ensure that the candidate system is exactly the system that was assessed.
- **Verify.** For each system in use during an election, ensure before use that it is the same as a previously assessed system.

These basic measures, enabled by high-assurance systems techniques outlined above, can dovetail with other integrity measures used by elections organizations to certify systems and to protect the integrity of the elections data they produce.

### THE WAY FORWARD

Guided by these principles and our convictions surrounding them, the Open Source Digital Voting Foundation is building a meritocratic community, using principles of open source development to design and make the guidelines, specifications, and demonstration systems that honor our 7 principles of veracity assurance and provide a way forward for the facilitators of American voting systems in a digital society.

#### OSDV Mission Specifics

The mission of the Open Source Digital Voting Foundation is fourfold:

1. **Specify** the key elements of high veracity digital voting devices & services, which fosters high confidence usage of them, which in turn, yields trusted election processes and results;

---

<sup>10</sup> See *Lectio Reformo Plenus* soon at [www.osdv.org](http://www.osdv.org). We make the case that the open source design and development of digital voting technology is, in fact, the only way to ensure these principles. The business case for the vendors of voting technology cannot easily be made. There is a limited number of polling stations in the United States (see *Footnote 9*), and although this may amount to 2-3 million devices, that is not large enough to justify the required R&D investment in building – from the ground up – high assurance systems devices pursuant to *Lectio Reformo*. However, the real revenue of any technology vendor is in service and support. Accordingly, we argue that placing the research and development for truly high veracity digital voting technology in the public trust, through an open source approach such as the OSDV, [a] frees the vendor to focus on their real business, [b] provides a public means to advance the state of digital voting technology that exceeds public expectations for trustworthiness, and [c] creates the most important system in a democracy – voting systems – by the people, for the people.

Indeed, some suggest that voting technology, systems, and services should be the province of the Government. We believe the market, and in this case, the power of the open source approach in a non-profit community setting incorporating the best and the brightest, can provide the best, most expeditious, most cost effective, and most publicly vetted results. The Government is free to adopt these results, and we will certainly earn their certification. And in our best realization of the mission, vendors will freely adopt the open source technology and build world class voting machines and services.

2. **Develop** and publish for public review and comment open specifications for the confident and transparent use of digital equipment & services deployed for voting;
3. **Build** a test bed system and service, widely available as a demonstration and educational tool, suitable for production use in polling and voting for private or public elections at the choosing of anyone; and
4. **Demonstrate** the effectiveness and utility of the guidelines, specifications, and demonstration systems and services for use by federal, state, and local election officials who [a] procure digital voting devices & services, [b] certify the same for use, and [c] conduct elections using digital voting devices & services; as well as for such officials or third parties who audit elections and their results.

## IN SUMMARY

The fastest growing problem with U.S. elections today is digital voting. Americans found a way past the “hanging chad,” but confidence in the way we vote is now at risk from computerized voting systems that were supposed to be the way forward. Increasing numbers of precincts are using computers to run elections – those representing over 60% of the nation’s voters have introduced new technologies since 2000. Yet we’re seeing more, not fewer problems. We’ve witnessed incidents ranging from wrongly recorded votes, to no way to recount, and even security lapses that can open the door to election fraud. But nearly all of these problems lie in basic technical aspects and procedures that can be successfully resolved first, before tackling any questions of optimal system design.

*Lectio Reformo* provides seven (7) principles of digital voting veracity assurance (DIVA), including: *Comprehension, Purpose, Specificity, Compatibility, Assurance, Certification, and Transparency*. We further believe there is a core set of design principles that must be adhered to in order to honor and protect these seven principles.

Further pursuant to *Lectio Reformo* it is essential to *first* produce specifications and guidelines that apply to *any and all* systems – *especially those already in place and likely to persist for some time to come*. And then, and only thereafter, should attention be trained on what digital systems for voting can and should look like, strictly guided by these principles. Guided by the principles herein, we intend to fully research, detail, vet, and pursue the realization of the root solution to restoring trust in voting systems in a digital age. To do so, we are building a community in the spirit of open source projects – that is the *Open Source Digital Voting Foundation (OSDV)*.

OSDV will advance open source digital voting, not because we believe open source is the only way, but because it is a very helpful approach and methodology and one that puts the results in the public trust freely accessible to all. *Lectio Reformo* does *not* advocate the elimination of the commercial sector pursuit of voting technology; on the contrary, OSDV hopes to support and partner with vendors. The mission of the OSDV is to specify, develop, and demonstrate “best practices” guidelines, tools, and systems for high assurance digital voting.

OSDV is a breakthrough organization that intends to bring together the best and brightest in technology and policy into a synergistic, meritocratic community focused on designing and building a high assurance open source digital polling/election service. The resulting guidelines, specifications, and fully functional demonstration service will be publicly available and ultimately freely adoptable as an educational tool, test-bed, and production ready service for polling and elections – private or public.

**E. John Sebes**

**Gregory A. Miller**

March, 2007