**E2E VIV Project Talking Points**

* *For Internal E2E VIV Project Use Only - Please Do Not Distribute –*

*Release 1.0 - December 14, 2013*

1. **In short form: What is this project about? What will you do?**The project is called *End-to-End Verifiable Internet Voting: Specification and Feasibility Assessment Study (E2E VIV Project)* and will examine a form of remote voting that enables a so-called “end-to-end verifiability” (E2E) property. A team of experts in computer science, usability, and auditing together with a selection of local election officials from key counties around the U.S. will assemble for this study. The project involves system specification and testing only. There will be no system development in this phase beyond mockups to help us test usability.
2. **In long form: What is this project about?**The E2E VIV Project focuses on development of a set of specifications for an end-to-end verifiable online voting process that could serve both disabled and remote absentee voters and that can stand up to adversarial real-world attack.   
     
   We will break the stalemate in communication and dialogue surrounding Internet voting technology development that exists between the best and brightest election technology experts in this country, and the dedicated, deeply experienced election officials who work tirelessly to enfranchise our citizens.   
     
   In the current climate of economic austerity, innovation in elections is rare. Our election officials are trapped in a technology no-man’s land of ongoing support payments for outdated voting systems, compounded by no means of certifying new voting systems they would like. These systems they envision aren’t even for sale. As a result, email has become the default stopgap method for moving ballots online, but it does not provide any of the benefits that a secure, full-featured voting system would provide and email is especially weak on security. We need to examine new and better ways to use technology to meet specific voting needs, for example, that of the remote overseas citizen or military voter.  
     
   This project brings election officials together with technologists to specify a Verifiable Internet Voting system that operates in an End-to-End manner – one that can stand up to the security challenges posed by the open Internet in a unique way – and one that is not afraid to be open and transparent for testing.   
     
   Usability and accessibility of the specified system is on par with security in importance. One without the other is useless in the voting scenario. (Working together in this diverse and unexpected team combination will serve to open a dialogue that has long simmered with misunderstandings). By bringing together a diverse and disparate team, we will promote dialogue that has long simmered with misunderstanding.
3. **Why is this project significant?**The significance of this project will be in its ability to break open the conversation and include all sides in a constructive project to openly examine and review what is really needed by voters and election officials, and to determine whether this form of voting can meet those needs and still guarantee security of the ballot. Equally important, it will identify associated tradeoffs and shortcomings that represent the diverse range of values we hold dear in our elections.   
     
   Our elections industry is not keeping up with the demand for innovation. This kind of paradigm-shifting development is uncommon, but you will find it out there in pockets – at the grassroots level. Without a great market, innovation comes to a standstill. We hope this will be a step to bringing new life into system/app development in elections.
4. **Everyone throws around “E2E”, but what is it really?**The term E2E is often used casually without precision. E2E-verifiability is considered a *property* of an election and for the purposes of this study, an E2E-verifiable election has two important components: first, that voters can individually check that their ballots are cast as they intend; and second, that anyone can check that all of the cast ballots have been accurately tallied.
5. **What is different here?  What is new?  Why would we even try such a thing?**There is a justifiably negative reflex response to Internet voting:  it takes all of the problems with current remote voting systems and adds all of the problems and security vulnerabilities of the Internet.    
     
   In this study, we aim to examine and potentially make the case that use of the Internet enables and facilitates the introduction of E2E-verifiability and that the benefits of E2E-V may be able to overcome the vulnerabilities introduced by using the Internet.   
     
   No participant on this project discounts the concerns of voting over the Internet, nor do they view E2E-verifiability as a magic sauce that makes the Internet secure. Nevertheless they believe that E2E-V warrants examination in regards to the properties it achieves. These properties are achieved even when votes are cast on untrusted devices like PCs and transmitted over an untrusted medium such as the Internet.
6. **Are you attempting to make a “secure” Internet?**This project does *not* attempt to make the Internet secure. Instead, E2E-V negates many (although not all) of the risks of voting via the Internet while introducing substantial new benefits that are not found in currently-deployed voting systems.
7. **What are the goals of the project?**The E2E VIV Project has 3 main goals:
   1. *Usability / Accessibility*: The specification for the system must start from a demand for usability and accessibility; this project will delineate and assess the E2E-verifiable voting protocol with usability and accessibility foremost in mind and determine if it meets requirements.
   2. *Security*: We aim to determine an optimal specification for a remote, end-to-end, verifiable Internet Voting (IV), one which will guarantee an acceptable level of security to enable geographically dispersed voters, specifically overseas and military voters, to utilize this method of voting, confident that their ballots are counted as cast, and to offer a method for signaling any suspicion that it is not, thereby enabling reparative action.
   3. *Testing*: The project must go beyond claiming the IV system to be secure; it must demonstrate that fact. The very difficult question of whether one can provide reasonable evidence for IV security will be addressed as we aim to propel understanding and awareness of this question – and its answer. Alongside this, it is our objective to set a new example, and a new standard for open testing and evaluation in the arena of IV. [This is, of course, exactly what we achieve with E2E-verifiability. Voters and observers need not depend upon our assertions that the system has been adequately tested but can instead perform their own external validation of correct system performance.]
   4. An additional benefit of the project is to embark on a constructive and shared working project that changes the tone of the dialogue between technologists, election officials, and some IV advocates that in past years has become increasingly frustrating and at times, even hostile..
8. **Is this a “capitulation” of sorts? Aren’t you all staunchly opposed to Internet Voting?**Voting integrity advocates are not against any form of Internet voting. But they do insist upon voting systems that can be demonstrated, openly tested, and proven to protect a voter’s ballot, specifically, proven secure and then audited. Whether there is a form of Internet Voting that can do that remains an open question. That is the question we will tackle: can an E2E-verifiable remote voting solution achieve ballot security and at that same time be considered usable?   
     
   This project represents a constructive action to change exactly this idea that there *is* something to capitulate on. It is wrong to characterize this as a battle and the aggressiveness of many advocates and opponents has not served the election community.   
     
   Election officials and scientists involved in elections share these goals: that voting systems can be proven secure, auditable, verifiable, and accessible.   
     
   This project is evidence that the needs and requests of election officials to explore optimum ways of serving remote voters are of deep concern to the scientific community, that they have a great motivation to address these questions when given a constructive opportunity to do so, and that they would like to work together, not at opposite ends, to examine the possibilities in this realm.
9. **What do you say to your colleagues involved in election integrity?  
   *WE ARE*** the colleagues involved in election integrity. There is nothing irresponsible about research working to specify a system that can be tested as secure before using it.   
     
   What ***IS*** irresponsible is selling an untested system with claims that it is secure, when that has never been proven. What is totally unhelpful is the hostility of some advocates who claim that IV is secure for voting when it has not been proven as such.   
     
   It’s time to change the conversation. This effort attempts to bring a diverse working group together to examine the open questions we share.
10. **Do you approve of what election vendors are currently doing in the arena of IV?**Unfortunately, among the current vendors, there is no great example of open, successful testing that demonstrates a secure IV system exists. One organization tried, OSDV, and failed quite miserably. The rest have kept their claims and left the demonstration of security up to our imaginations and the willingness of people to believe what they claim to be true, but have never proven true in a testing environment.
11. **Can it really be that there is a secure IV system? Doesn’t this say, you believe that it is possible?**If E2E Verifiable Internet Voting is a possible answer, or a step toward one, we want to find out. If it works, it will answer the needs of many voters and election officials. If not, we will still gain great and specific knowledge about the shortcomings, which can be further acted upon in the future. One of our major goals is to determine specifically whether there is a secure E2E VIV system or else to demonstrate specifically why the answer is “no”.
12. **Is there a hidden motive? Are you really out to torpedo IV?**Absolutely not. We are committed to searching for solutions that will solve the problems facing overseas, military, and disabled voters. We aim to move the IV discussion forward in a constructive manner and do so by taking real action. Real work will be done to achieve the objectives of the project. We hope people will take this opportunity for positive, constructive action. If E2E VIV is not possible, we want to know exactly why it is not possible. If it is possible, then we would plan to move forward.
13. **Do you plan to build the system you specify?**We are on step one in an examination of whether one day this might be possible. Our current plan is to examine the potential for an E2E VIV remote voting system together with election officials, taking into close account their needs and the needs of disabled voters. If a system can one day be developed based on these principles, then we want to know. We need the answers that this project will bring before we can say whether we, or anyone, will build any new system. A viable outcome of this study with respect to security, auditability, and usability will enable development efforts to ensue.
14. **What do you expect to accomplish? What will be produced from this effort? And who will it help?**In this study, we aim to examine the benefits of E2E-verifiability and whether they may be able to overcome the vulnerabilities introduced by using the Internet in voting.  
       
    We expect to produce a report presenting a set of system specifications to create a secure E2E VIV system, a set of testing specifications to demonstrate the security, a set of guidelines for system usability, accessibility, and testing. Additional topics and analyses may be considered and discussed in the report, such as legal and administrative challenges, and ballot secrecy, privacy, and confidentiality.
15. **What constitutes project success?**We would consider it a success if we can specify a system and testing for a usable, secure E2E verifiable remote voting technology. We will answer the question as to whether this works and identify strengths and weaknesses and reasons to pursue or not pursue this approach to remote and/or disabled citizen voting.  
      
    If we determine that the technology is weak and should not be developed, that would be a different outcome, but also with many useful implications.   
      
    Beyond judging the outcome – the fact that we are taking a research and testing-based approach to a question/problem that has been “in stalemate mode” will result, we believe, in stimulating election development overall. This goes back to the earlier comment about the elections industry being starved. The industry is operating in a traditional paradigm with a few vendors being the only ones that can survive – albeit with outdated, expensive, hardware-oriented solutions.
16. **How will a “successful project” move forward?**If the E2E VIV system we specify is deemed successful, it will motivate follow-on actions. Part of the project is indeed to examine this question closely and develop a business plan for this type of success, if it ensues. The Democracy Fund is very kindly kick-starting what may be a longer project, but any development follow on will require new funding sources.
17. **What next? What comes after?**The team on the project would like to make the system open-source. That is a way to not only to move it forward, but also to keep it moving forward.  
      
    In addition, we would seek new partners to develop a prototype system and once again challenge it to testing. We would examine the outcomes and carefully determine if in actuality it performed as expected and stood up to the security challenges. If in the long-run, we end up with a system that can be deployed in elections offices around the country, supported and maintained as an official system, it would represent a major step forward in absentee and accessible voting.
18. **What is the timeframe?**It is an 18-month total timeframe. The project is underway and will be complete by May 2015.
19. **When do you think you will have a sense of the success or failure?**There is no failure unless we are unable to produce a report, which is unlikely. The success of the project lies in sufficiently addressing a question that has not been answered due to an inability or unwillingness to discuss in a collaborative and open fashion.
20. **Is this project simply limited to military and overseas voters plus voters with disabilities or is this *really* a plan to introduce Internet voting to everyone via the backdoor?**For us, the project is limited to military and overseas voters plus voters with disabilities. We are not advocating this method of voting for all. Frankly, we are not advocating anything. We are executing a research project.
21. **Why should we introduce this to military and overseas voters when their turnout is so small? Does the effort and expense match the potential number of voters you seek to address?**Good questions – please see Q23.
22. **What would you say to those election officials and other key stakeholders in the** election community who simply are opposed to this type of technology regardless of your findings?  
    Each person has a right to his or her opinion. Everyone in America is skeptical of how we can protect information flowing over the Internet. It is an educated approach to question it. Being against this form of voting regardless of the findings? If not for scientific reasons then, there may also be policy reasons. We are not out to change people’s opinions. We are taking a research-based approach to a set of open questions for which election officials and our voting population would like answers.
23. **How do you know this technology will bring in more voters to the process? After all, other ‘improvements’ in the voting process for military and overseas voters have not had a significant impact on overall voter turnout.**We don’t know that it will. And we don’t know that it won’t. This is a baby step toward maybe, one day, finding out. There are Internet Voting attempts that have indicated decline in turnout – but there is nothing truly definitive yet. If it results in a decline in turnout, it would die a natural death.
24. **This is a tall order in this time frame. Are you concerned about being able to thoroughly analyze this topic and complete the project on time?**We can do it. Our technical team has decades of man/woman years of experience in E2E technology, system usability, and accessibility. We are not starting at zero – we are collecting together, using what we know and going forward from there. That makes it possible. We believe in the possible.
25. **What if your team cannot work together due to differences of opinion?**Now wouldn’t that be fun to write about? Nice try.   
      
    No one joined this team with any intention other than wanting to find the common ground and work together from there. It’s nothing short of exciting. And don’t miss how exceptional it is. Would that others would do the same.
26. **What and how should we communicate with the rest of the world about the results of the project?**The results will be published and available to all. That is a precept of the agreement with the Democracy Fund. Nothing gets buried. You’ll be the first to know!
27. **Who is on the team?**One of the highlights of this project is the team, which brings together people who have not been working especially constructively together over the last years – election officials and computer scientists involved in election integrity.   
      
    This diversity provides a great opportunity to build or rebuild a dialogue and tackle an open question.   
      
    There are several teams within the team: a Technical Team, a Usability Team, a Research Team, a Management Team. We will have an Advisory Council, which will enable others to communicate their ideas and thoughts and which will provide for an official means of doing so.

**Technical Team**:

**Dr. Josh Benaloh**

Senior Cryptographer, Microsoft Research

**Dr. Doug W. Jones**

Associate Professor, Department of Computer Science, University of Iowa

**Dr. Aggelos Kiayias**

Associate Professor, Computer Science and Engineering, University of Connecticut

**Dr. Olivier Pereira**

Professor, Institute of Information and Communication Technologies, Electronics and Applied Mathematics, Ecole Polytechnique de Louvain

**Dr. Poorvi Vora**

Associate Professor, Department of Computer Science, The George Washington University

**Dr. David Wagner**

Professor, EECS Computer Science Division, University of California Berkeley

**Dr. Dan Wallach**

Professor, Department of Computer Science, Rice University

**Usability Team:**

**Keith Instone**

User Experience Consultant

**Jim Tobias**

Inclusive Technologies

**Election Auditing**

**Dr. Philip Stark**

Professor and Chair of Statistics, University of California Berkeley

**Testing Specifications and Determinations**

**Dr. Duncan Buell**

Professor of Computer Science and Engineering, University of South Carolina

**Andrew Regenscheid**

Mathematician, National Institute of Standards and Technology

**Board of Advisors**

**Dr. Ben Adida**

Engineering Lead, Square

**Rachel Bohman**

Former Hennepin County Elections Manager (Minnesota)

**Dr. Michael Clarkson**

Assistant Professor of Computer Science, The George Washington University

**Dr. J. Alex Halderman**

Assistant Professor of Computer Science and Engineering, University of Michigan

**Candice Hoke**

Professor of Law, Cleveland State University

**Dr. Ron Rivest**

Vannevar Bush Professor of Computer Science, Massachusetts Institute of Technology

**Noel Runyan**

Primary Consultant, Personal Data Systems

**Dr. Peter Ryan**

Professor in Applied Security, University of Luxembourg

**Dr. Barbara Simons**

Fellow of Association for Computing Machinery (ACM), Fellow of the American Association for the Advancement of Science

**Dr. Vanessa Teague**

Research Fellow, Department of Computing and Information Systems, University of Melbourne

**John Wack**

Voting Systems Standards, National Institute of Standards and Technology

**Local Election Officials:**

**Dana Debeauvoir**

Travis County Clerk (Texas)

**Mark Earley**

Leon County Supervisor of Elections (Florida)

**Dean Logan**

Los Angeles Registrar-Recorder/County Clerk (California)

**Roman Montoya**

Deputy County Clerk, Bernalillo County (New Mexico)

**Tammy Patrick**

Federal Compliance Officer Maricopa County (Arizona)

**Overseas Vote Foundation Support Team**

**Susan Dzieduszycka-Suinat**

President and CEO

**Dr. Judith Murray**

Research Consultant

**Paul McGuire**

Legal Counsel and Secretary of the Board

**Richard Vogt**

Treasurer and Chief Financial Officer