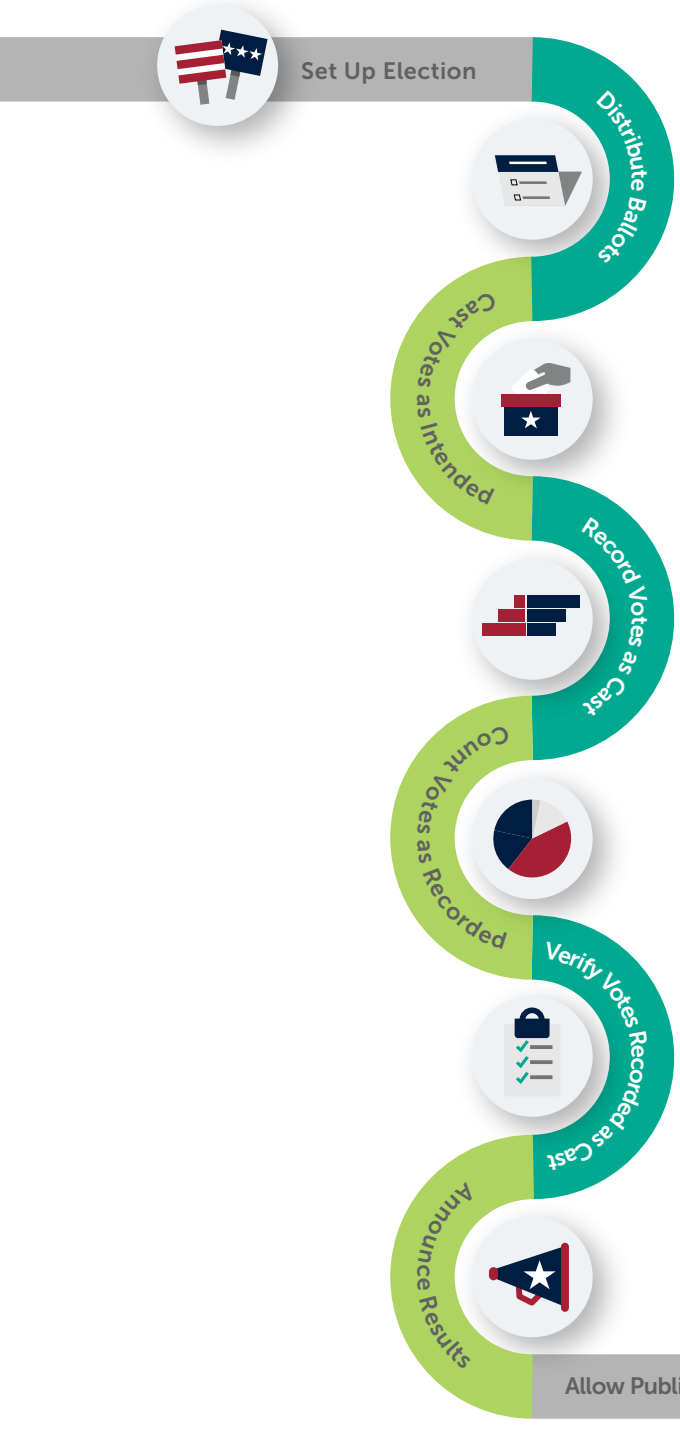

THE FUTURE OF VOTING

END-TO-END VERIFIABLE INTERNET VOTING

SPECIFICATION AND
FEASIBILITY ASSESSMENT STUDY

A PROJECT OF **U.S. VOTE FOUNDATION**
WRITTEN AND PRODUCED BY **GALOIS**

U.S. VOTE FOUNDATION

U.S. VOTE FOUNDATION
SUSAN DZIEDUSZYCKA-SUINAT, PRESIDENT AND CHIEF EXECUTIVE OFFICER
JUDY MURRAY, PH.D.

GALOIS
JOSEPH R. KINIRY, PH.D.
DANIEL M. ZIMMERMAN, PH.D.

DANIEL WAGNER, PH.D.
PHILIP ROBINSON
ADAM FOLTZER
SHPATAR MORINA

July 2015

INTRODUCTION

Societies have conducted elections for thousands of years, but technologies used to cast and tally votes have varied and evolved tremendously over that time. In 2015 many of our essential services have moved online, and some people want elections to follow this trend. Overseas voters are particularly interested in an online approach, as their voting processes can require additional effort and suffer from long delays.

Internet voting systems currently exist, but independent auditing has shown that these systems do not have the level of security and transparency needed for mainstream elections. Security experts advise that end-to-end verifiability—lacking in current systems—is one of the critical features needed to guarantee the integrity, openness, and transparency of election systems.

In this report, we examine the future of voting and the possibility of conducting secure elections online. Specifically, we explore whether End-to-End Verifiable Internet Voting (E2E-VIV) systems are a viable and responsible alternative to traditional election systems.

This project combines the experience and knowledge of a diverse group of experts committed to election integrity. The technical team, comprised of academic and scientific specialists, has long term, proven experience in end-to-end verifiable systems, cryptography, high-assurance systems development, usability, and testing.

INTERNET VOTING TODAY

Internet voting was first proposed over thirty years ago. Since then, many governments and businesses have created Internet voting technologies that have been used to collect millions of votes in public elections.

However, computer scientists, cryptographers, and cybersecurity experts warn that no current Internet voting system is sufficiently secure and reliable for use in public elections.

Part of the problem is that existing systems do not allow third parties to observe the election system and independently verify that the results are correct. In fact, most vendors explicitly forbid such oversight.

SECRET

No existing commercial Internet voting system is open to public review. Independent parties cannot verify that these systems function and count correctly, nor can they audit and verify election results.

INSECURE

Elections for public office are a matter of national security. Researchers have shown that every publicly audited, commercial Internet voting system to date is fundamentally insecure.

NO GUARANTEES

No existing system guarantees voter privacy or the correct election outcomes. Election vendors are rarely held liable for security failures or election disasters.

END-TO-END VERIFIABILITY

An end-to-end verifiable voting system allows voters to:

- check that the system recorded their votes correctly,
- check that the system included their votes in the final tally, and
- count the recorded votes and double-check the announced outcome of the election.

An Internet voting system that is end-to-end verifiable is an **E2E-VIV** system.

The concept of E2E-VIV is decades old. However, most of the required computer science and engineering techniques were impractical or impossible before recent advances. Designing and building an E2E-VIV system in the face of enormous security threats remains a significant challenge.

INTERNET VOTING REQUIREMENTS

Internet voting must be end-to-end verifiable. It must also be secure, usable, and transparent.

SECURE

Security is a critical requirement for Internet voting, and also one of the most challenging. An Internet voting system must guarantee the integrity of election data and keep voters' personal information safe. The system must resist large-scale coordinated attacks, both on its own infrastructure and on individual voters' computers. It must also guarantee vote privacy and allow only eligible voters to vote.

USABLE

Nearly all E2E-VIV protocols designed to date focus on security at the expense of usability. Election officials and voters will not adopt a secure but unusable system. Cryptographers have started to recognize usability as a primary requirement when designing new protocols, and usability is a serious challenge that any future work in this area must address. Any public Internet voting system must be usable and accessible to voters with disabilities.

TRANSPARENT

It is not enough for election results to be correct. To be worthy of public trust, an election process must give voters and observers compelling evidence that allows them to check for themselves that the election result is correct and the election was conducted properly. Open public review of the entire election system and its operation, including all documentation, source code, and system logs, is a critical part of that evidence.

End-to-end verifiability, security, usability, and transparency are only four of many important requirements. This report contains the most complete set of requirements to date that must be satisfied by any Internet voting system used in public elections.

RECOMMENDATIONS

The five key recommendations of this report are:

1. Any public elections conducted over the Internet must be end-to-end verifiable.

2. No Internet voting system of any kind should be used for public elections before end-to-end verifiable in-person voting systems have been widely deployed and experience has been gained from their use.

3. End-to-end verifiable systems must be designed, constructed, verified, certified, operated, and supported according to the most rigorous engineering requirements of mission- and safety-critical systems.

4. E2E-VIV systems must be usable and accessible.

5. Many challenges remain in building a usable, reliable, and secure E2E-VIV system. They must be overcome before using Internet voting for public elections. Research and development efforts toward overcoming those challenges should continue.

It is currently unclear whether it is possible to construct an E2E-VIV system that fulfills the set of requirements contained in this report. Solving the remaining challenges, however, would have enormous impact on the world.

OUTCOMES

The report contains the following:

REQUIREMENTS

We identify a comprehensive set of requirements for an E2E-VIV system.

ARCHITECTURES

We review a variety of ways to build, deploy, and run an E2E-VIV system and the associated engineering issues.

ENGINEERING AND TECHNOLOGY

We present a set of rigorous engineering methodologies, technologies, and tools that are fundamental to building a correct and secure E2E-VIV system.

SECURITY

We lay the foundation for developing a cryptographic system that reflects the ideal functionality of an end-to-end verifiable system, and discuss the technologies that should be used to implement that system.

USABILITY

We present the results of an initial usability study showing that significant effort is needed to develop usable E2E-VIV systems.

ACKNOWLEDGMENTS

This project and report would not have been possible without the commitment and tireless hard work of the team at Galois, Inc. Our special acknowledgment and appreciation goes most especially to Joseph Kiniry, who brought his decades of knowledge, skill, experience, and leadership to the project, broadened its scope and led the technical team and writing; and with him, the Galois team members Daniel Zimmerman, Daniel Wagner, Philip Robinson, Adam Foltzer, Shpatar Morina, and Leah Daniels. We are indebted to CEO Rob Wiltbank for the Galois engineering contribution and the long leash he gave to this project.

We would also like to thank the research and technical members of the E2E-VIV Project Team for their contributions to this project from its conception to its completion, with special thanks to Josh Benaloh, Candice Hoke, Keith Instone, David Jefferson, Doug Jones, Aggelos Kiayias, Judy Murray, Ron Rivest, Barbara Simons, and Poorvi Vora.

Equally vital and integral to this report were the reflections, insights and advice from election officials who joined our team, most especially Lori Augino, Judd Choate, Dana Debeauvoir, Mark Earley, Stuart Holmes, Dean Logan, Tammy Patrick, Roman Montoya, and Lois Neuman.

We also thank Sean Beggs, Randall Trzeciak, and Andrew Wasser, Carnegie Mellon University, Heinz College Master of Information Systems Management for their support through the CMU ISM Capstone Program.

We are grateful for the generous financial support of the Democracy Fund, as well as their support of collaborative efforts in the realm of civic tech development.

SUSAN DZIEDUSZYCKA-SUINAT
PRESIDENT AND CHIEF EXECUTIVE OFFICER
U.S. VOTE FOUNDATION

ABOUT U.S. VOTE FOUNDATION

U.S. Vote Foundation (US Vote) and its initiative, Overseas Vote, are dedicated to bringing a comprehensive range of best-in-class voter services to U.S. citizens residing within the U.S., living abroad or serving in the military. US Vote's exclusive Voter Account application supports voters' ongoing participation in the electoral process. Through its hosted systems program, US Vote helps states, campaigns and voter outreach organizations offer their own customized online voter services. US Vote is poised to respond to the growing need for research and development of alternatives to polling place voting. U.S. Vote Foundation is a 501(c)(3) nonprofit, nonpartisan public charity incorporated in Delaware.

For additional information on U.S. Vote Foundation, please visit www.usvotefoundation.org.

For additional information on the Overseas Vote Initiative, please visit www.overseasvote.org.

ABOUT GALOIS

Galois specializes in the safety, security and reliability of critical hardware and software systems where failure is unacceptable. We apply a solid foundation of mathematics, applied formal methods, and science to advance cryptography, language design, scientific computing, software correctness, mobile security, cyber-physical systems, and computer security.

For additional information on Galois, please visit www.galois.com.

ABOUT THE DEMOCRACY FUND

The Democracy Fund invests in organizations working to ensure that our political system is responsive to the public and able to meet the greatest challenges facing our nation.

For additional information on the Democracy Fund, please visit www.democracyfund.org.

WITH GENEROUS SUPPORT FROM THE

DEMOCRACY FUND

OF, BY, AND FOR THE PEOPLE