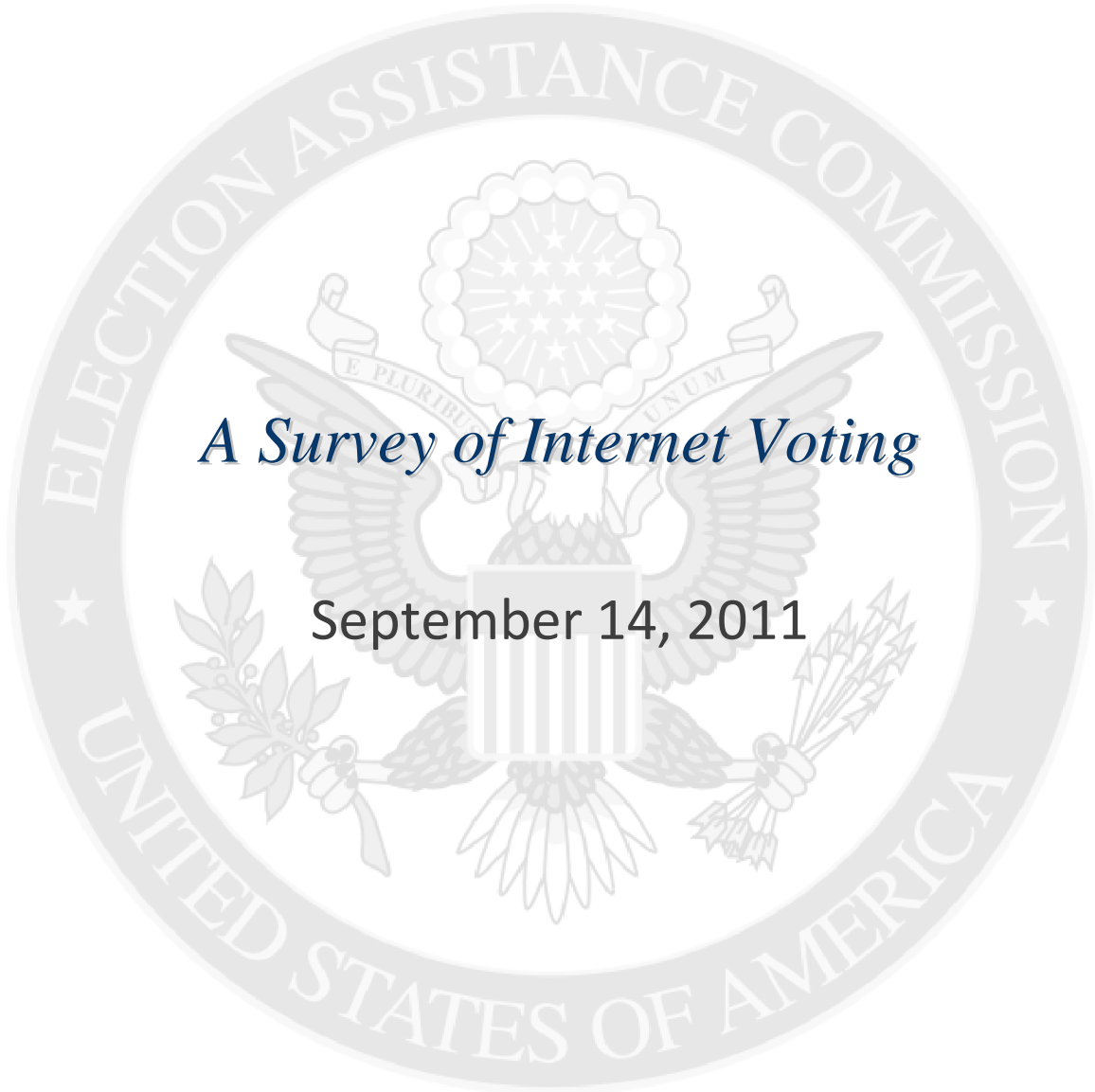


U.S. Election Assistance Commission

Testing and Certification Technical Paper #2



A Survey of Internet Voting

September 14, 2011

Voting System Testing and Certification Division

1201 New York Avenue, NW, Suite 300

Washington, DC 20005

www.eac.gov

Acknowledgements:

The Election Assistance Commission would like to thank the following individuals for their contributions: Jussi Aaltonen, Chris Backert, Daniel Bierer, Mark Brewer, Ian Brightwell, Christian Bull, Craig Burton, Susanne Caarls, Michel Chevallier, Aaron Contorer, João Falcão e Cunha, Rota Danilo, Sean Dean, Paul Docker, Andreas Ehringfeld, Raenette Gee, Jackie Harris, Kimberley Kitteringham, Robert Krimmer, Manuel Kripp, Tarvi Martens, Ardita Driza Maurer, Cathy Mellet, Daniel Muster, Mark Novitski, Sal Peralta, Piet Pont, Jordi Puiggali, Michael Remmert, Andrew Scallan, Paul Stenbjorn, Craig Stender, and Beth Ann Surber.

The workproduct that follows represents the work of the EAC staff and does not represent a policy decision by the Commission.

Comments on this publication can be submitted to:
U.S. Election Assistance Commission
Attn: Voting System Testing and Certification Division
1201 New York Ave, NW, Suite 300, Washington,DC 20005

Table of Contents

Section 1 Introduction	6
Overview	6
Legislative Mandate	7
Scope.....	7
Internet Voting Channels	8
Terminology	10
Methodology.....	11
Structure	12
Section 2 United States Projects	14
Alaska.....	14
Arizona	15
2000 Democratic Primary	15
2008 & 2010 General Elections.....	16
Democrats Abroad	18
District of Columbia	19
Honolulu.....	21
Michigan.....	22
Okaloosa Distance Balloting Project (ODBP)	23
Oregon	27
Secure Electronic Registration and Voting Experiment (SERVE)	29
West Virginia.....	32
Voting Over the Internet (VOI)	34
Section 3 European Projects	40
Austria.....	40
Estonia.....	43
Finland.....	46
France.....	48
Netherlands.....	52
Norway.....	54
Portugal.....	57

Spain.....	58
Sweden.....	60
Switzerland.....	62
Swiss Federal Mandates	62
Geneva.....	63
Neuchâtel.....	65
Zurich.....	67
United Kingdom	68
2002 Pilot Projects	69
2003 Pilot Projects	74
2007 Pilot Projects	78
Section 4 Canadian Projects	80
Halifax.....	81
Markham.....	82
Peterborough	84
Section 5 Oceanic Projects	86
Australia	86
State of New South Wales	88
Victoria	93
Section 6 Observations.....	96
Implementation	99
Standards and Requirements	101
Addressing Risk	103
Final Thoughts.....	104
Appendix A: Bibliography.....	105
Appendix B: Project List.....	111
Appendix C: ODBP Kiosk Equipment	116
Appendix D: ODBP System Architecture	117
Appendix E: SERVE Voting Protocol.....	118
Appendix F: SERVE System Architecture	119
Appendix G: VOI System Diagram	120

Appendix H: VOI Voter Instructions	121
Appendix I: Austrian System Architecture	122
Appendix J: Estonian System Diagram	123
Appendix K: Netherlands' Voting Card (2004)	124
Appendix L: Netherlands' Voting Card (2006).....	125
Appendix M: Swiss Election History.....	126
Appendix N: Geneva Voting Card.....	127
Appendix O: AEC System Architecture	128
Appendix P: New South Wales System Architecture	129
Appendix Q: Data Tables.....	130
Endnotes.....	136

Section 1 Introduction

Overview

This report presents a broad review of the Internet voting systems used in elections from January 2000 through November 2011. The U.S. Election Assistance Commission (EAC) conducted this study to collect information to use as guidance in the development of electronic absentee voting guidelines. The knowledge gained from examining the system architectures, the standards for designing and/or testing these systems and how system risk was evaluated and managed provides valuable insight based on actual experience.

Several countries began conducting studies and preparing to field voting pilot projects in the late 1990s, including the U.S., the Netherlands, the United Kingdom, Switzerland and Sweden. By the mid- to late 1990s, inexpensive personal computing technology and Internet access had become widely available in most developed countries. The ability to connect directly with consumers revolutionized the way commercial services were provided in the private sector. These developments spurred governments to consider how information technology might be used to perform various public functions more effectively and efficiently. Reducing the cost of elections, improving voter turnout, and making voting more accessible for absentee voters and voters with disabilities are among the objectives frequently cited for piloting Internet voting.

In the U.S., government sponsored Internet voting projects have predominantly focused on absentee voting. The Uniformed and Overseas citizens Absentee Voting Act (UOCAVA) protects the right to vote absentee in federal elections for members of the Uniformed Services stationed away from their place of voting residence and for citizens living abroad. UOCAVA designates the Secretary of Defense as the executive agent for implementing its provisions. The Department of Defense (DoD) Directive 1000.04 created the Federal Voting Assistance Program (FVAP) to administer the Act on behalf of the Secretary.¹

UOCAVA was enacted before the advent of universally available global communications networks. Consequently, it prescribes the use of U.S. domestic and military mail systems and, by extension, foreign postal systems for the worldwide distribution of election materials. By the mid-1990s it became apparent that mail transit time and unreliable postal delivery posed significant barriers for many UOCAVA citizens, preventing them from successfully exercising their right to vote. To address this issue, in October 1997 FVAP met with state and local election officials to discuss a project to test the feasibility of using electronic delivery as an alternative to postal mail.² The State and Local Government Alliance was established to work with FVAP to plan this effort. By

Section 1: Introduction

1999 the groundwork was laid to conduct a small pilot project for the 2000 General election.

In that same year, 1999, two major studies were conducted in the U.S. -- the California Internet Voting Task Force and the National Workshop on Internet Voting. Both studies concluded that the use of the Internet poses a potential threat to election integrity.^{3,4}

Internet security is a technical and policy issue that persists today. The questions raised more than a decade ago still pertain:

- Given that no system can be 100% secure, what level of risk can be accepted for such a fundamental democratic process as voting?
- How can a sponsor considering Internet voting measure the level of risk associated with various methods and technologies?
- How can a sponsor create and implement standards for this technology and reliably test to those standards?

This document attempts to address these questions and presents the experiences of each project sponsor.

Legislative Mandate

Since the implementation of FVAP's Voting Over the Internet (VOI) pilot in 2000, the U. S. Congress has expressed its continuing support for pilot projects to explore ways to overcome the voting barriers faced by UOCAVA voters, particularly those in the military. The National Defense Authorization Act of 2005 directed the EAC to create electronic absentee voting guidelines and to assist FVAP in carrying out a demonstration project. The Conference Report accompanying this bill states: "The conferees recognize the magnitude of the technical challenge associated with ensuring the security of electronic voting using the Internet."⁵

The National Defense Authorization Act of 2009 required the EAC to submit a report containing a detailed timeline for the establishment of these guidelines. In response, the EAC, in conjunction with FVAP and the National Institute of Standards and Technology (NIST), created a "roadmap" for establishing these guidelines.⁶ One of the roadmap activities is to research and compile information about the experiences of other countries that used Internet voting. In the interest of providing as complete a picture as possible, the EAC included U.S. Internet voting projects in the research scope. The results will serve as reference material to the Technical Guidelines Development Committee and other stakeholders involved in the creation of electronic absentee voting guidelines.

Scope

The primary objectives of this research were to identify:

Section 1: Introduction

- the standards used for the development and testing of Internet voting systems;
- the level of risk assumed and how it was estimated; and
- the entity that decided what was the acceptable level of risk.

To provide context for this information, a brief description of each project is provided. As an aid to making comparisons between and among the projects, a summary table is provided at the beginning of each project. Table 1-1 provides a sample table with a definition of the descriptors used.

Table 1-1 Summary Table

Sponsor:	The entity sponsoring the project
Election Type:	Type of election (e.g., Federal, local, etc.)
Date or Voting Period:	The day or days on which voting took place
Target Population:	The intended users of the system
Channel:	The method of Internet voting used
Technology Provider:	The entity providing the system
Channel Protection:	The mechanism used to protect ballot data during transmission
Participating Voters:	Number of voters who cast ballots
Authentication:	The mechanism used to verify voter identity

Internet voting systems created exclusively for military and overseas voters are not the sole focus of this report. Internet voting systems intended for domestic or other types of voters may be applicable to military and overseas voters and details about those systems are included.

Internet Voting Channels

The term “Internet voting” is used to refer to many different methods, or channels, of voting. What these channels have in common is the use of the communications connectivity and protocols provided by the Internet. The Internet is a global information system composed of hundreds of thousands of independent computers and networks that are logically linked together by a common set of communication standards, procedures and formats. It provides the connectivity, message routing and end-to-end communication services that enable the development of a constantly evolving array of information services.⁷

Figure 1-1

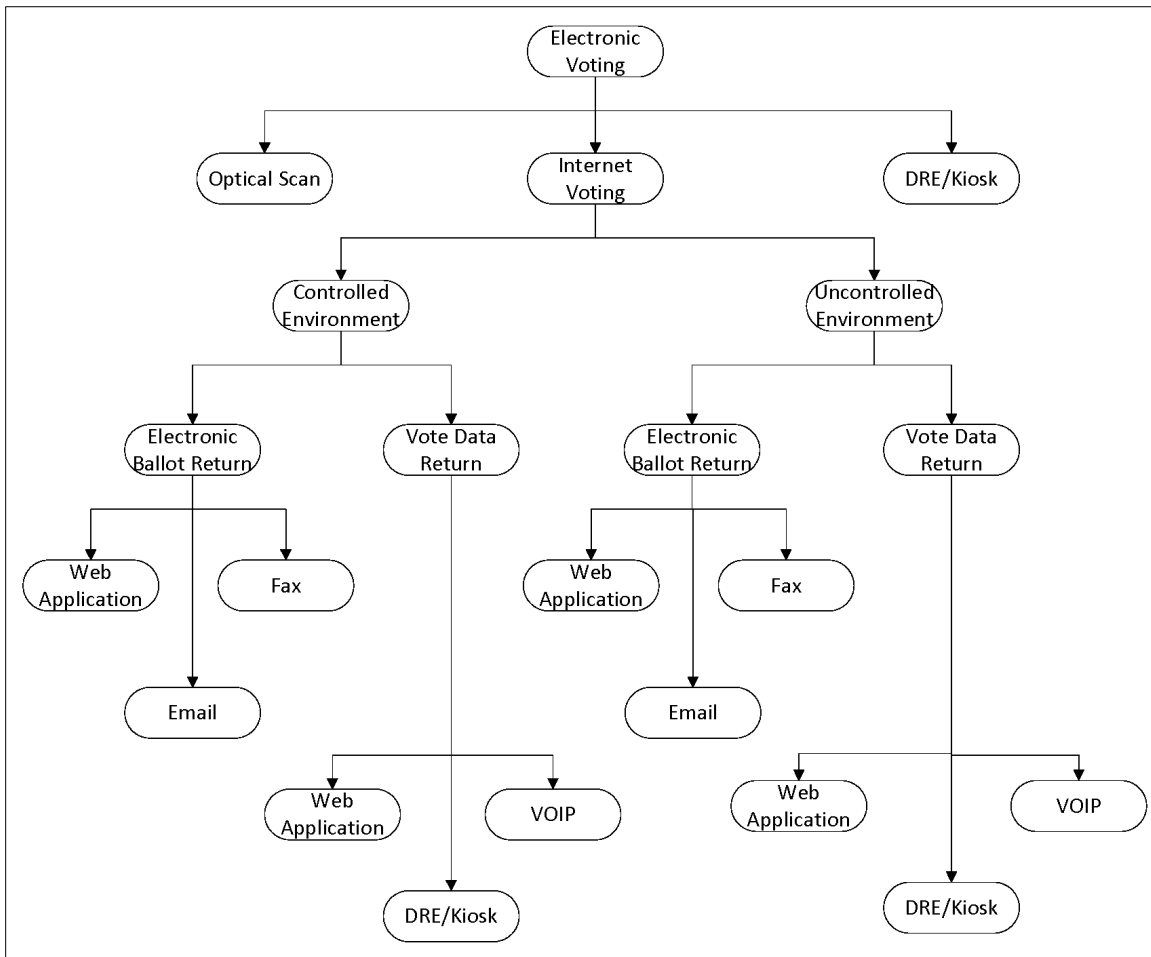


Figure 1-1 classifies Internet voting as a subset of electronic voting. For purposes of this research, an Internet voting system was defined as any system where the voter’s ballot selections are transmitted over the Internet from a location other than a polling place to the entity conducting the election. Hence the term “remote electronic voting” is often used as a synonym for Internet voting. Based on this definition, blank ballot distribution systems, online marking systems and public switched telephone network (PSTN) systems are not considered Internet voting systems.

As indicated in Figure 1-1, the remote voting location can be either a controlled or an uncontrolled voting environment. A controlled environment means that the voting platform (i.e., computer used for voting) was supplied by, and was under the control of, the entity conducting the election. An uncontrolled environment means the voter supplies the computer used for voting, which might be their personal computer, their workplace computer, or any other public computer.

There are two forms in which the voter’s ballot selections can be returned: electronic ballot return, where the entire ballot document, including the voter’s

Section 1: Introduction

sections, is transmitted; or vote data return, where only the voter's selections are transmitted.

There are three channels, or methods, for electronic ballot return:

- a web-based communications application which uploads a digital representation of a voted ballot (e.g., pdf, jpeg, png) file to a website;
- digital facsimile, where a voted ballot is scanned and transmitted as a graphics file; and
- email, where a digital representation (e.g., pdf, jpeg, png) of a voted ballot is transmitted via email.

There are also three channels, or methods, for presentation of the ballot and vote data return:

- a web browser or computer application which the voter executes to display the ballot, record selections and transmit selections;
- a DRE or kiosk connected to the Internet to transmit vote data; and
- a Voice Over Internet Protocol (VOIP) approach for the voter to access the ballot, record selections and transmit selections.

This report includes examples of Internet voting systems using all of the above channels of electronic ballot return and vote data return except systems utilizing email and fax technology.

Terminology

In an effort to standardize the terminology used in this report, Table 1-2 provides definitions of frequently used terms.

Table 1-2 Frequently Used Terms

Term	Definition
<i>Continuous use system</i>	Internet voting system used by a location in three or more elections. A pilot project system can become a continuous use system by being adopted as a regular voting channel.
<i>Controlled environment</i>	Voting location, voter authentication, and voting platform are provided by the entity sponsoring the election. The sponsor provides supervision at the voting site.
<i>Electronic voting</i>	Any form of vote tabulation and vote submission utilizing electronic components. Also notated as E-Voting, eVoting, and Evoting.

Section 1: Introduction

<i>Internet voting</i>	Any form of ballot delivery where a voter's ballot selections are returned to a tabulation system via the Internet. Also notated as I-Voting, iVoting, and ivoting.
<i>Kiosk-based Internet voting</i>	Internet voting conducted from a voting platform provided by sponsor.
<i>Pilot project</i>	Internet voting technology implemented by election officials in a specific location during a specific timeframe, and used by a specific population of voters, to experiment with new technology and/or voting systems.
<i>Remote electronic voting</i>	The submission of a voter's ballot selections over public infrastructure from a location other than a polling place. Remote electronic voting can be performed from systems in controlled and uncontrolled environments. Also notated as distant electronic voting.
<i>Uncontrolled Environment</i>	The voter provides the voting platform (e.g., personal PC) at a location of their choosing. In person authentication is not used, but electronic authentication to access the system is necessary.

In an effort to compare dissimilar information, an organizational scheme was developed to assist with the comparison of projects. The full list of included projects is located in Appendix B. Each instance of Internet voting is referred to as a project, encompassing the sponsor, location, system and year, presented as:

- Project;
- Sponsor;
- Location;
- System;
- Year.

Methodology

The EAC gathered information for this project by reviewing newspapers, books, website articles, scholarly journals, and government documents from a variety of sources. In-person interviews, telephone interviews, and email correspondence with election officials and voting system manufacturers provided the EAC with first-hand information about many of the projects discussed. Additionally, the EAC consulted various U.S. government sources throughout the course of this research. Those sources include members of the U.S. Election Assistance Commission; Federal Voting Assistance Program; Federal Election Commission;

Section 1: Introduction

the National Institute of Standards and Technology; and state and local government officials. Data collection for this report began in December 2009 and ended August 2011. This report presents a broad review of the Internet voting systems used in elections from January 2000 through November 2011.

Throughout this document, readers will notice instances when the EAC was unable to locate information related to the scope of the report. In some Internet voting projects, standards were not used and the concept of risk was not discussed. Sponsors have different methods for conducting elections. The goal of this research was to collect, understand, and present information; therefore, the EAC does not endorse, approve, or disapprove of any project or system discussed. When the EAC was unable to locate information on a specific item or topic, the section containing the item includes a sentence stating: “The EAC was unable to obtain this information.” Gaps in data are expressed in this manner to give an accurate representation of the information collected. If additional or updated information is available regarding a project listed in this report, please contact the EAC.

Often, the entity assuming risk for a project is cited in this document as the project sponsor. The level of risk assumed for a project is listed using the metrics each sponsor used during the risk assessment process. Risk is an inherently difficult concept to quantify and can be expressed in several ways. Information regarding a project’s level of risk, regardless of the metric used, is included in this report.

Structure

The projects using Internet voting included in this report are organized according to geographical regions:

- United States;
- Europe;
- Canada;
- Oceania.

Obtaining access to and gathering the information about the projects in this report was difficult and required the resources of a federal agency. At publication, the EAC could not locate detailed information about Internet voting systems or projects in Latin America, Africa, South America or mainland Asia. Table 1-3 lists the projects not included due to insufficient information or scheduled to occur after the publication of this report.

Section 1: Introduction

Table 1-3 Projects not Included in Report

Year	Location	Election Type
1996	U.S. (Reform Party)	Presidential Primary
2002	New Zealand	General Election
2004	Madrid, Spain	Municipal Election
2005	Mendoza, Argentina	State Medical Board
2007	Philippines	General Election
2010	Barcelona, Spain	Municipal Election
2010	Burlington, ON, Canada	Municipal Election
2010	Gujarat, India	Municipal Election
2011	Norway	Federal Election
2012	Arizona, U.S.	General Election
2013	New Zealand	Local Election
2014	Victoria, Australia	State Election

Section one provides the background information and scope of this report. Sections two through five discuss the Internet voting projects organized by geographical region. Section six presents observations and identifies the need for future research based on the data collected. The appendices contain diagrams for individual systems that were too large to be included in the body of this report.

Section 2 United States Projects

Alaska

Sponsor:	Alaska Republican Party
Election Type:	Party Primary
Date or Voting Period:	January 24, 2000
Target Population:	Alaskan Republican Party members
Channel:	Uncontrolled>Vote Data Return>Web Application
Technology Provider:	VoteHere Inc.
Channel Protection:	The EAC was unable to obtain this information
Participating Voters:	35 ⁸
Authentication:	One-factor: eight-digit PIN

Alaskan voters are faced with unique geographical challenges, highlighted in a New York Times article, which stated: “In some parts of Alaska, about the only way to get to a voting booth in January is by dogsled.”⁹ In an effort to increase turnout among Alaskan voters in geographically isolated areas, the Alaskan Republican Party contracted with a voting system vendor, VoteHere Inc. On January 24, 2000, voters cast ballots in a “non-binding presidential preference vote.”¹⁰ Congressional members of Alaska located in Washington, D.C., were offered the opportunity to participate in the pilot.¹¹ The Alaskan Republican Party’s Chairman, Randy Ruedrich, said the pilot project was “not a grand success, but a great experiment.”¹² One of the problems affecting turnout cited by Ruedrich was that “rural Alaska connectivity to the Internet was much less than the state average.”¹³ Information on the underlying technology of the system is not available because “there was no scientific plan for a meaningful evaluation of the Alaska straw poll.”¹⁴

Standards Used

The EAC was unable to obtain this information.

Level of Risk Assumed

The EAC was unable to obtain this information.

Entity Assuming Risk

The Alaskan Republican Party assumed the risk for the pilot project.

Arizona

Internet voting technology was used in three elections in Arizona: the 2000 Democratic Primary, the 2008 General Election and the 2010 General Election. One voting system was used for the 2000 Democratic Primary. A different voting system was used for the 2008 and 2010 General Elections. These were two distinct systems, in two distinct projects, with different sponsors.

2000 Democratic Primary

Sponsor:	Arizona Democratic Party
Election Type:	Party Primary
Date or Voting Period:	March 7, 2000
Target Population:	Registered Democratic Party members
Channel:	Uncontrolled>Vote Data Return>Web Application
Technology Provider:	election.com
Channel Protection:	HTTPS, shared administrative passwords
Participating Voters:	39,942 ¹⁵
Authentication:	One-factor: PIN

The 2000 Arizona Democratic Primary occurred on March 7, 2000. Registered Democrats in Arizona “cast legally-binding ballots for their presidential primary across the Internet from anywhere in the world.”¹⁶ In *The Security of Remote Online Voting* Daniel Rubin stated the “2000 turnout was barely 10% and the Internet votes only accounted for 46% of the votes cast.”¹⁷

The Democratic Party of Arizona used election.com to provide and administer the voting system for the election. Problems experienced while using the voting system on voter PCs during the election included: malfunction of antiquated browsers, operating system incompatibility, and administrative issues (e.g., loss of the PIN required for accessing the voting system).¹⁸

Standards Used

“The election was not a public election, so the voting system was not subject to the voting standards that apply to systems used for public elections.”¹⁹

Level of Risk Assumed

Although a level of risk was not identified, some form of penetration testing occurred. Daniel Seligson of Stateline.org stated: “Security was tight, despite an

Section 2: United States Projects

effort by a group hired by party officials to try and hack into the system to test its integrity.”²⁰

Entity Assuming Risk

The Arizona Democratic Party assumed the risk for the pilot project.

2008 & 2010 General Elections

Sponsor:	Arizona Secretary of State’s Office
Election Type:	General Election
Date or Voting Period:	November 4, 2008, November 2, 2010
Target Population:	UOCAVA Voters
Channel:	Controlled>Electronic Ballot Return>Web Application/Email/Fax
Technology Provider:	Arizona Secretary of State’s Office
Channel Protection:	128-bit SSL
Participating Voters:	The EAC was unable to obtain this information
Authentication:	Two-factor: Username/Password and electronic representation of voter’s signature

The Arizona Secretary of State’s Office implemented an Internet voting system for the 2008 General election, which was used again in 2010.²¹ The Arizona Secretary of State’s Office developed the voting system, which utilized a variety of industry standard technologies including: Microsoft .Net 3.5, Microsoft SQL Server, and 128-bit SSL. Voters received their ballot by postal mail, email or fax. After marking selections, the voter scanned the ballot and affidavit and uploaded them to the Arizona Secretary of State’s servers.²² The ballots were transcribed onto a replacement ballot for tabulation on the local tabulation device.²³ The voting process for Arizona’s web-based system is:

- 1) The voter contacted the Arizona SOS’s Office and requested to participate in the program.
- 2) The county of the registered voter received an email notification of the voter’s request from the SOS’s office.
- 3) The county authorized the voter to participate and created an account for the voter.
- 4) The election office sent the voter an email containing credentials and system instructions.

Section 2: United States Projects

- 5) A ballot was sent to the voter via mail, email, or fax.
- 6) The voter printed the ballot, if necessary.
- 7) The voter made ballot selections and scanned the ballot into their personal computer.
- 8) The voter navigated to the URL provided in the email and entered the credentials.
- 9) The voter uploaded the scanned ballot and signed affidavit to the Arizona SOS website.
- 10) The voter and appropriate county official received a confirmation email regarding the ballot submission.
- 11) The county official downloaded the ballot from the Arizona Secretary of State's Office for transcription, canvass and tabulation.

Standards Used

The EAC was unable to obtain this information.

Level of Risk Assumed

The EAC was unable to obtain this information.

Entity Assuming Risk

The Arizona Secretary of State's Office assumed the risk for the pilot projects.

Democrats Abroad

Sponsor:	Democrats Abroad
Election Type:	Party Primary
Date or Voting Period:	February 5-12, 2008
Target Population:	Members of the Democratic Party living abroad
Channel:	Uncontrolled>Vote Data Return>Web Application
Technology Provider:	Everyone Counts
Channel Protection:	HTTPS, client side vote encryption using RSA
Participating Voters:	All voting channels: 23,105 ²⁴
Authentication:	One-factor: PIN and username

Democrats Abroad is the overseas branch of the United States Democratic Party. Democrats Abroad contracted with San Diego based company, Everyone Counts, to provide the voting system for the Party Primary. From February 5-12, 2008, U.S. citizens living overseas were offered the opportunity to vote in an online, global primary to choose the Democratic nominee for President.²⁵ Democrats Abroad reported that “Online ballots were cast from 164 countries and territories, from Antarctica to Zambia.”²⁶

Democratic Party members located outside of the United States were required to register to participate with Democrats Abroad by February 1, 2008. After registration, voters received an e-mail containing a ten-digit ballot number and an eight-digit PIN. To vote, a voter navigated to the Democrats Abroad website, and logged in with the ballot number. Each user supplied additional personal information before accessing a Java applet to begin the voting process.²⁷ Users without the Java Runtime environment were offered an HTTPS and an HTML interface.²⁸

The final results for the 2008 Democrats Abroad Global Primary were not released until February 21, nine days after the voting period concluded. The initial reporting of the election results was incorrect; however, the error was resolved and was cited to be the result of "a programming error in a spreadsheet column."²⁹

Standards Used

The EAC was unable to obtain this information.

Level of Risk Assumed

The EAC was unable to obtain this information.

Entity Assuming Risk

Democrats Abroad assumed the risk for the pilot project.

District of Columbia

Sponsor:	District of Columbia Board of Elections and Ethics
Election Type:	General Election
Date or Voting Period:	Scheduled for November 2, 2010 General Election
Target Population:	UOCAVA voters
Channel:	Controlled>Electronic Ballot Return>Web Application
Technology Provider:	Open Source Digital Vote Foundation
Channel Protection:	SSL/TLS
Participating Voters:	0
Authentication:	One-factor: Name, Address, and PIN ³⁰

The District of Columbia Board of Elections and Ethics (DCBOEE) planned to launch a “Digital Vote by Mail” system during the 2010 General Election for absentee, military and overseas voters. The system was composed of two distinct elements: an online blank ballot distribution system and a system designed to allow for the return of voted ballots. The ballot return system provided voters with the opportunity to upload voted ballots in PDF format to the DCBOEE’s servers via the Internet. According to the TrustTheVote project, the Open Source Digital Voting Foundation provided technological support for the project and “...acted in the capacity of a technology provider – somewhat similar to a software vendor, but with the critical difference of being a *non-profit R&D organization*.”³¹

Beginning September 28, 2010, the DCBOEE subjected the voting system to a six-day testing period for members of the public to discover vulnerabilities. This testing period was open to all individuals requesting credentials to participate. During this time, a group of Ph.D. students from the University of Michigan, with the assistance and support of a faculty member, were able to discover and exploit multiple vulnerabilities in the DCBOEE’s voting system.³² The vulnerabilities allowed for the University of Michigan team to take control of the DCBOEE voting system and modify ballots, install a “back door”, and collect username and password combinations.³³

After DCBOEE officials were made aware of the attack on the voting system, the system was removed from operation and the testing period was suspended. On

Section 2: United States Projects

October 8, 2010, the online blank ballot distribution system was brought back into operation. Due to the test results, the portion of the system designed to return voted ballots was not used in the 2010 General Election.

Standards Used

The DCBOEE's *An Overview and Design Rationale Memo* highlights a number of standard security practices used in the Digital Vote By Mail system including: HTTPS, PGP encryption, and digital signatures.³⁴ The document highlights other standard counter-measures, including: network segmentation, network throttling, and defense against Distributed Denial of Service (DDOS) attacks. The EAC was unable to locate specific standards used in the creation of the voting system.

Level of Risk Assumed

The DCBOEE performed a risk assessment prior to the implementation of the system and it is included in the DCBOEE's *An Overview and Design Rationale Memo*.³⁵ This document outlines a Threat Model comparing the identified threats of D.C.'s Digital Vote by Mail (D.C.dVBM) voting system to current methods of "paper return and email return."³⁶ The document includes a matrix summarizing the threats to the system and describes recommended countermeasures.

The DCBOEE attempted to avoid introducing new threats to the voting system, especially threats not present in the current vote by mail process. This is evidenced by the following excerpt from the DCBOEE:

Besides these two effects on threats in existing digital ballot return, the threat-related goals for D.C.dVBM are:

- to not worsen existing threats,
- to not introduce new classes of threats,
- to introduce new threats only if they are analogous to existing threats,
- to not convert existing "retail" threats to "wholesale" threats,
- and in general:
- to maintain the existing VBM operational model,
- to maintain the existing VBM threat model.³⁷

Entity Assuming Risk

The District of Columbia Board of Elections and Ethics assumed the risk for the system.

Honolulu

Sponsor:	City of Honolulu
Election Type:	Neighborhood Board Election
Date or Voting Period:	May 6, 2009
Target Population:	General Electorate
Channel:	Uncontrolled>Vote Data Return>Web Application
Technology Provider:	Everyone Counts
Channel Protection:	SSL ³⁸
Participating Voters:	154,000 voters were registered; unable to locate turnout
Authentication:	One-factor: Password

The City of Honolulu held its Neighborhood Board Election on May 6, 2009, via an “all-digital voting system.”³⁹ This voting system included web-based Internet voting and telephone voting. The city of Honolulu is located on the island of Oahu which is divided into 33 Neighborhood Boards. The Neighborhood Board is a voluntary entity under the Mayor’s purview. The Neighborhood Board operates in an advisory capacity to the city, county, and state governments. The operations of the Board are paid for by the government, but the elected officials do not receive a salary.

In previous elections, the Election office used the postal system to conduct the election. The Neighborhood Board cannot use the State’s electronic voting technology to conduct elections. Since the election was for Neighborhood Board members, Hawaii’s public election laws, which require a voter-verified paper audit trail, did not apply to the system.⁴⁰ Everyone Counts provided the technology, allowing voters to cast ballots from their home computers.

Standards Used

The County of Honolulu published a Request for Proposal (RFP) for *On-line Voting Services for the 2009 Neighborhood Board Elections* on February 23, 2009.⁴¹ The RFP specified requirements for hardware, software, security, availability and many other procurement-related items. The “...primary goal of this RFP is to have an on-line voting system offered to the voters. However, a supplemental alternative – either through paper votes or by telephone, etc- shall also be submitted for evaluation and must work in conjunction with this main on-line method.”⁴²

The RFP notes that the “...Offeror’s system must be able to handle a minimum of one-third (1/3) of the eligible voters attempting to log in simultaneously.”⁴³

Section 2: United States Projects

Details regarding alternative ballot languages, the number of personnel with access to the back-end of the system, voter interaction with the system, voter privacy requirements, accessibility, the Offeror's employees, and the initial demonstration of the system are in the RFP.

An addendum was released detailing discussions between prospective bidders and the City of Honolulu.⁴⁴ The City of Honolulu required the on-line voting system to meet HAVA standards.⁴⁵ Additional information regarding Logic & Accuracy (L&A) Testing and post election auditing was included in the document. The addendum included a reference to using an ISO 27001 certified data center to host the Internet voting system.⁴⁶

Level of Risk Assumed

The City of Honolulu stated that the Offeror must provide an alternative method of voting that "should be at least as safe as the all-paper method used in the 2005 election."⁴⁷

Entity Assuming Risk

The City of Honolulu assumed the risk for the system.

Michigan

Sponsor:	Michigan Democratic Party
Election Type:	Party Primary
Date or Voting Period:	February 7, 2004
Target Population:	Members of the Michigan Democratic Party
Channel:	Uncontrolled>Vote Data Return>Web Application/Fax
Technology Provider:	election.com
Channel Protection:	The EAC was unable to obtain this information
Participating Voters:	46,543 ⁴⁸
Authentication:	One-factor: voter code, place and date of birth

In 2004, the Michigan Democratic Party (MDP) conducted a Presidential Primary via the Internet. The MDP administered the election and provided each voter with a unique identifier and PIN number. To participate, an individual applied for an absentee ballot or voted in person on Election Day. The absentee ballot application was accessed on the MDP website. Several candidate campaigns distributed the absentee ballot application to supporters. The application was

Section 2: United States Projects

completed online or printed and returned to the MDP by mail or fax.⁴⁹ Upon receipt, MDP staff checked the application against the state voter file to ensure that the application was returned by a registered Michigan voter. Voters could then vote via the Internet.⁵⁰

Standards Used

The EAC was unable to obtain this information.

Level of Risk Assumed

With encryption and firewalls in place, the executive chairman of the Michigan Democratic Party deemed the safeguards as adequate.⁵¹

Entity Assuming Risk

The Michigan Democratic Party assumed the risk for the system.

Okaloosa Distance Balloting Project (ODBP)

Sponsor:	Okaloosa County Supervisor of Elections
Election Type:	General Election
Date or Voting Period:	October-November 2008
Target Population:	Military and Overseas voters
Channel:	Controlled>Vote Data Return>DRE/Kiosk
Technology Provider:	Scytl
Channel Protection:	VPN, SSL, multiple layers of encryption and digitally signed data
Participating Voters:	93
Authentication:	Two factor: In person identification with photo ID, digital certificate

The Supervisor of Elections in Okaloosa County, Florida, fielded a small pilot project for the 2008 General Election, known as the Okaloosa Distance Balloting Pilot (ODBP). There are numerous military installations representing every branch of the military based in Okaloosa County. There are over 20,000 active duty service members and dependents registered to vote in the county. To avoid the security concerns raised by the SERVE project (see SERVE section), voting was conducted in a controlled voting environment using a computer provided and administered by the local election office.

Section 2: United States Projects

The voting sites, called kiosks, were set up in hotels in three overseas locations: Mildenhall, England; Ramstein, Germany; and Kadena, Japan. These locations were selected because they have U.S. military installations with high concentrations of Okaloosa voters. The sites in England and Germany were open for a 10 day period prior to the election and closed 2 days before Election Day (October 24th through November 2nd). The Japan site was open for only 2 days, due to a last minute issue that required finding a new location.

The ODBP architecture was composed of three segments: kiosk sites, the central servers hosted in a commercial data center, and the Okaloosa elections office server and voter registration database. Appendix C shows the physical equipment used at the kiosk sites. The database was hosted in the county data center. As indicated in the system architecture in Appendix D, all communications between the various elements of the system were provided by VPN connections through the Internet.

The configuration of the Voter Authentication System consisted of a hardened laptop computer, a printer, a bar code scanner and a smartcard reader. This system was used to verify the voter's eligibility; print the state required Voter Certificate; and extract specified data elements from the voter registration database to encode a smart card used to activate the voting session at the voting laptop. The Voter Authentication System was connected to the Okaloosa voter registration database via the Internet to update voter history data in real time.

The voting laptop configuration consisted of a touch screen connected to a laptop computer, a smartcard reader and a printer. The entire Operating System (OS) the voting laptop used (e.g., voting specifications) was written to read-only media, known as the Live CD. The laptop was connected through a VPN to the central server.

When a voter arrived at the kiosk site, they presented a photo ID to the kiosk worker, who validated the voter's eligibility to vote using the voter registration database. If verified, a Voter Certificate was printed so the voter could sign the state oath. This document contained data such as voter name and address, date of birth, election identifier, voter registration number, precinct number and ballot style. Selected data elements were captured in a bar code, which was scanned by the kiosk worker to write the required voter credentials and ballot style information on a smart card.

The voter inserted the smart card in the reader attached to the voting computer to initiate the voting session. The smart card data were transmitted to, and validated by, the central server that returned an electronic ballot, along with the digital certificate issued for that voter. The voter made their selections and received a paper record of their choices to compare with the summary screen display. If the voter was satisfied with their choices, they touched the "Vote" button. The voting software encrypted the voter's selections, applied the voter's digital signature using their digital certificate and transmitted the voter's

Section 2: United States Projects

selections to the central server. A receipt was printed with a randomly generated code that the voter could use after the election to see if his ballot was counted. Removal of the smart card closed out the voting session. The voter returned the smart card to the kiosk worker along with the paper record, which was stored in a receptacle and returned to Okaloosa County as part of the election records.

Since the kiosks were set up in hotel rooms, the only available physical security measure was to lock the door when the kiosk was not in operation. Consequently, the Live CD with the voting application and all other sensitive materials were removed each day when kiosk operations ended and kept under the physical control of the kiosk workers. Each morning the kiosk workers checked the tamper evident seals on the computers, initialized the Voter Authentication System, checked the integrity of the Live CD by verifying the hash, rebooted the voting laptop and established the VPN link.⁵²

The central server hosted the ballot database, delivered the correct ballot style to the requesting voter, stored the encrypted voted ballots in an electronic ballot box, and delivered the ballot box to the Okaloosa County Canvassing Board upon request after the close of the election. The central server also maintained detailed audit logs of all system transactions and events. The system software installed on the central servers was the same software tested, certified and digitally signed by the Florida Bureau of Voting Systems Certification.

The computer designated as the “mixing server” in the architecture diagram is a critical component of the voting system. This server was operated and administered by the election office staff. Before the start of voting, the mixing server was used by the Okaloosa Canvassing Board to generate a public/private key pair for the election. The public key was used to encrypt the ballots cast by the voters. The private key was used at the end of the election to decrypt the ballots. The private key was divided into shares, which were distributed to the Canvassing Board members and then the key was erased from the system. This ensured ballot contents could not be viewed during the voting period. Multiple shares were required to reconstruct the key, so no single person could decrypt the ballots when the voting period closed. After this process was completed, the mixing server was stored in the office vault.

At the end of the voting period, the bridge laptop was used to download the encrypted ballot box from the central server. The ballot box file contained the ballots, which were individually encrypted and digitally signed by the voters. Then, the entire file was wrapped in another layer of encryption and transmitted. This file was manually transferred to the mixing server by means of a USB memory stick because this server was required to be isolated from any network. The mixing server verified that the encrypted ballot box file had not been tampered with or corrupted during transmission. Then the Canvassing Board reconstructed the private key and authorized the decryption and tabulation of the ballots. This process breaks the correlation between voters and

Section 2: United States Projects

ballots and mixes the ballot order to preserve anonymity. A tabulation report was produced and the results manually uploaded to the county election management system.

Standards Used

The Florida Administrative Rule 1S-2.030 Electronic Transmission of Absentee Ballots authorized the project.⁵³ This rule permits a supervisor of elections to provide overseas voters the option of voting by secure remote electronic transmission if certain requirements were met. These requirements included the submission of a project plan for approval by the State Division of Elections. The rule also specified the information that the plan had to include. The project plan had to be approved by the Florida Division of Elections before the project could proceed.⁵⁴

In addition, the system was required to be tested and certified for use by the Florida Bureau of Voting Systems Certification. The test plan incorporated the administrative rule requirements, the applicable Florida Voting System Standards, and additional security standards defined to cover elements of the system not addressed by the Florida standards.⁵⁵

Level of Risk Assumed

The security controls implemented in the ODBP project were defined following an ISO 27001 risk management approach. Florida Administrative Rule 1S-2.030 was the starting point for security requirements. After identifying the vulnerabilities and security threats to which the system could be exposed, a set of physical, logical and procedural security controls were defined to prevent the materialization of threats or to mitigate their impact. These security controls are summarized in Section 11 of the June 19 project plan.⁵⁶ A third party independent team of voting system experts conducted a software review and analysis of the security architecture of the system and several elements were modified based on the findings of this group.⁵⁷

The level of risk assumed by ODBP personnel was very low due to a number of factors:

1. The system was designed with robust, multi-layered security architecture.
2. The system utilized successfully implemented technologies used in a number of previous government elections.
3. All ballot data was encrypted and digitally signed while in transit and in storage.
4. All system communication was performed over dedicated virtual private networks, established with digital certificates at both ends for strong authentication.
5. Two levels of firewalls blocked public access to the system.

Section 2: United States Projects

6. Alternative communications paths were available to mitigate against denial of service attempts.
7. The voting sites were under the administrative control of the election office.
8. The integrity of kiosk voting software was validated each day.⁵⁸

Entity Assuming Risk

The Supervisor of Elections of Okaloosa County and the Florida Secretary of State's office assumed the risk for this project. The elections supervisor was the system proponent and the state tested and certified the system for use.

Oregon

Sponsor:	Independent Party of Oregon
Election Type:	Party Primary
Date or Voting Period:	July 2010
Target Population:	Members of the Independent Party of Oregon
Channel:	Uncontrolled>Vote Data Return>Web Application
Technology Provider:	Everyone Counts
Channel Protection:	The EAC was unable to obtain this information
Participating Voters:	~2,500 ⁵⁹
Authentication:	One-factor: Voter code

In July 2010, the Independent Party of Oregon (IPO) held a statewide Party Primary Election using Internet voting technology provided by Everyone Counts.⁶⁰ The election involved candidates for Governor of Oregon; for U.S. Representative in three of Oregon's five congressional districts; and for Oregon Senator or Representative in 56 out of 90 state legislative districts. Minor political parties in Oregon typically nominate candidates via caucus or conventions. In this instance, the Independent Party of Oregon selected candidates via a primary election. Citing an increase in membership, the IPO sought a nominating method that would involve more party members than those that would attend a caucus or convention. Over 55,000 IPO members received a notice via postal mail that included unique codes assigned by Everyone Counts.⁶¹ Each voter could log-in to a website operated by Everyone Counts to cast a ballot online.

Standards Used

A state council of three people evaluated proposals based on a variety of factors, including cost, security, ease of use, vendor experience. System requirements of the internet voting system included:

- 1) Vendor accepted total responsibility for administering the system and is able to provide clear and accurate reporting of all activity related to the election.
- 2) Only party members registered by a certain date were eligible to participate.
- 3) System must be accessible through any computer with http access.
- 4) System must deliver correct ballot to voters by district.
- 5) Each voter may have one and only one vote for each office.⁶²

Ultimately, the IPO selected Everyone Counts and its web-based Internet voting technology.⁶³

Level of Risk Assumed

The EAC was unable to obtain this information.

Entity Assuming Risk

An IPO member stated:

Everyone Counts bore the risk of systems failure on its own website and its software to count the votes. IPO bore the risk of educating the press and public to minimize voter confusion. It did so by publishing an online voting tutorial, by publicizing the primary in earned media, and by providing specific procedures for voters to report problems and for candidates to have an opportunity to contest the results before a retired judge who acted as a neutral to decide any candidate objections. No candidates, voters, or members of the public lodged any complaints about the conduct of the primary election.⁶⁴

Secure Electronic Registration and Voting Experiment (SERVE)

Election Type:	General Election
Date or Voting Period:	Scheduled for 2004 General Election
Target Population:	Military and Overseas voters
Channel:	Uncontrolled>Vote Data Return>Web Application
Technology Provider:	FVAP, Hart InterCivic
Channel Protection:	SSL 3.0 with session keys, and encrypted and digitally signed data (SHA1 with DSA)
Participating Voters:	0
Authentication:	Two factor: User name and password, X .509 digital certificate

Following the completion of the Voting Over the Internet (VOI) project in 2000, in the Fiscal Year 2002 National Defense Authorization Act (§1604 of P.L. 107-107:115 Stat.1277), Congress instructed the Secretary of Defense to carry out a larger demonstration project. The States of Arkansas, Florida, Hawaii, North Carolina, South Carolina, Utah, and Washington agreed to work with FVAP and ask counties to participate in the Secure Electronic Registration and Voting Experiment (SERVE) project for the November 2004 election. Fifty-five counties from Arkansas, Florida, Hawaii, North Carolina, South Carolina, Utah and Washington chose to participate. However, the SERVE project was cancelled before it was deployed due to security concerns raised by a group of computer scientists. These individuals publicly issued a critique of the system contending that the use of personal computers over the Internet could not be made secure enough for public elections and called for the project to be terminated.⁶⁵ The Department of Defense, citing a lack of public confidence in the system because of this report, decided that the project could not continue under these circumstances.

The SERVE architecture was a central hosting environment with distributed access from local election officials and voters using any computer that met the minimal compatibility requirements.⁶⁶ A system architecture diagram is located in Appendix F.

Nearly all system processing, except tabulation, was performed on the central server site. The system software consisted of eight integrated subsystems: Identification and Authentication; Common Services; Voter Registration; Election Administration; Ballot Definition; Voting; Download and Decryption; and Tabulation. Each participating local election jurisdiction (LEO) had a dedicated environment on the system to enable them to independently administer their own election processes from any workstation in their office.

Section 2: United States Projects

There was an SFTP connection with the voter registration database server for downloading the voter registration applications submitted on the system for processing by the LEO. Each LEO was provided a hardened laptop for the download, decryption and tabulation of ballots from the central hosting environment. Capabilities for local election officials included voter registration, election definition, ballot, ballot decryption, ballot tabulation, and voter history.

Voters were required to use a computer running a Windows Operating System with either Netscape or Internet Explorer as the web browser. The voter needed to have a SERVE digital certificate. System services for voters included: online voter registration and updating of voter information online; ballot delivery and vote selection; and review of their registration and voting status. When the voter finished making vote selections, the selections were transmitted to temporary storage in the cast vote record database on the central server.⁶⁷ A summary was sent back to the voter to confirm the vote selections as received by the cast vote record database were correct. Upon return of the confirmation message by the voter, the vote selections were permanently stored in the database on the central server until downloaded by the LEO.⁶⁸

SERVE established its own X.509 compliant certificate authority using VeriSign roaming certificates.⁶⁹ Personal digital certificates were issued to all system users – LEOS, voters, and system administrators. Machine certificates were provided for LEO servers exchanging non-ballot data with the central server and for all the central server elements. This provided a complete audit trail of all user transactions and all machine-generated events. A minimum of two LEO personal certificates plus a hardware token with a password were required for the use of the LEO laptop to download, decrypt and tabulate ballots.

If a voter had a Department of Defense (DoD) Common Access Card (CAC), they could use that credential to identify themselves to the SERVE system. Upon the system's verification of this credential against the DoD PKI Certificate Revocation List, the voter was issued a SERVE certificate for future system access. The reason for replacing the CAC with a SERVE credential was to enable voters to use any computer to access the system and not be restricted by needing a card reader. The roaming certificate was stored on the system and was accessed with the voter's user name and password. Voters who did not have a CAC card were issued a SERVE certificate by physically presenting themselves with a suitable identification document to a SERVE trusted agent. A diagram of this process is located in Appendix E.

Standards Used

The testing regimen planned for the SERVE system was a combined DoD Information Technology Security Certification and Accreditation Process (DITSCAP), National Association of State Election Directors (NASSED), and State of Florida certification and accreditation process. As was the case with the earlier

Section 2: United States Projects

Voting Over the Internet project (see VOI section), the available voting system standards did not include standards for the more advanced technologies employed, such as cryptography, digital certificates and the Internet. The SERVE project team began with the VOI testing requirements and expanded them to cover all the elements of the system security architecture and communications links.⁷⁰ In addition to the Florida Voting System Standards and the 2002 Federal Election Commission Voting System Standards, a variety of Federal Information Processing Standards (FIPS), ISO standards, the Open Web Application Security Project standards and Common Criteria Protection Profiles Guidelines were drawn upon to provide the system testing requirements. The results of the SERVE Threat Risk Assessment process identified areas where additional security testing was needed.

Level of Risk Assumed

The SERVE project used the Facilitated Risk Analysis Procedure (FRAP) methodology as the basis for its phased risk assessment activity. FRAP uses a diverse team of subject matter experts to identify the pool of risks and rank them in a comparative fashion. The process is not designed to create hard risk values but rather comparative risk qualifiers to give system designers and project managers the ability to focus on the risks with the highest priority for the project. While different teams of experts might assign different levels of risk ratings to risk elements, the design of the methodology causes the overall ranking of the risks to remain generally the same. Portions of the National Security Agency INFOSEC Assessment Methodology were employed to create information criticality ratings. NSA, as a detailed and systematic way of examining cyber vulnerabilities, developed this methodology. The results of the risk assessment were used in the system security architecture design phase and also factored into the system testing requirements.

As a generalized statement of the acceptable level of risk, the SERVE Report states, "At the very least, any new form of absentee voting should be as secure as current absentee voting systems."⁷¹ However, a risk assessment has not been performed on the by mail UOCAVA absentee process, so there is no baseline for making a comparison. The threat profile for voting by mail is significantly different than the threat profile for Internet voting.

Entity Assuming Risk

Different levels of risk applied to each of the entities participating in the project, depending on their system role. FVAP relied on due diligence of conducting a formal phased risk assessment throughout the system development cycle; monitoring and review of system development process; developing system security requirements to be responsive to risks; collaborative development of system requirements with states and counties; conducting thorough certification

Section 2: United States Projects

and accreditation testing for conformance to both functional and security requirements and doing third party penetration testing prior to deployment.⁷²

After deployment, the use of random third party penetration testing, continuous monitoring of system performance audit logs with pre-specified alarm conditions, and random third party review of system audit logs were planned as mechanisms to maintain awareness of the threat environment.

State election office due diligence consisted of relying on FVAP's due diligence; participating in the development of system requirements; participating in system design reviews; approving the system design; participating, reviewing and approving certification and accreditation testing and possibly doing their own acceptance testing; and participating in system administration decisions in the event of detected anomalous activity during the system's operation.⁷³

Local election office due diligence relied upon FVAP's and their State's actions, performing their own Logic & Accuracy testing, and adhering to system operating and security procedures.⁷⁴

Voters assumed the risk of keeping their personal computers free of malware, properly protecting their electronic credentials to prevent fraudulent use, reliable service from their ISP provider, and using an experimental system.

West Virginia

Sponsor:	West Virginia Secretary of State's Office
Election Type:	Primary and General Elections
Date or Voting Period:	Primary: May 11, 2010; General: November 2, 2010
Target Population:	West Virginia UOCAVA voters
Channel:	Uncontrolled>Electronic Ballot Return>Web Application/Email/Fax
Technology Provider:	Everyone Counts and Scytl
Channel Protection:	SSL ⁷⁵
Participating Voters:	Primary: 54 web-based votes cast ⁷⁶ ; General: 125 web-based
Authentication:	One-factor: Username/Password ⁷⁷

Anticipating the 2009 MOVE Act, West Virginia enacted the Uniform Services and Overseas Voter Pilot Program. This legislation required the Secretary of State to implement and evaluate an Internet voting pilot program for military and overseas voters.⁷⁸ West Virginia used a "comprehensive screening process" to

Section 2: United States Projects

contract with Scytl and Everyone Counts to provide the technology for the pilot project.⁷⁹ Five counties participated in the May pilot, and three additional counties participated in the November pilot. Each participating county independently selected one of the vendors pre-screened by the West Virginia’s Secretary of States’ Office. Table 2-1 associates each county to their technology provider:

Table 2-1^{80,81} County and Technology Provider

Date	County	Technology Providers
5/11/2010	Kanawha	Everyone Counts
5/11/2010	Jackson	Scytl
5/11/2010	Marshall	Scytl
5/11/2010	Monongalia	Everyone Counts
5/11/2010	Wood	Everyone Counts
11/2/2010	Mason	Scytl
11/2/2010	Monroe	Everyone Counts
11/2/2010	Putnam	Everyone Counts

West Virginia’s Pilot Program allowed for the use of email, fax, and web-based Internet voting.⁸² In order to cast a ballot using the web-based system the voter:

- 1) Submits a Federal Post Card Application (FPCA) or the West Virginia Electronic Voting Absentee Ballot Application.
- 2) Receives an email from either the county clerk or a voting system vendor which contains a username and URL for a website to access the ballot.
- 3) Logs into the website using the supplied credentials.
- 4) Makes ballot selections on the computer screen.
- 5) Selects the “Cast Ballot” button.
- 6) Receives a receipt code.

The receipt code is used to ensure the ballot is received and processed correctly by the voting system. The receipt code does not allow a voter to view their ballot once the ballot is cast.⁸³

The participating counties did not report any problems during the election with either vendor’s voting systems. Due to concerns discussed at the 2010 UOCAVA Solutions Summit and the unsuccessful test of the District of Columbia’s Internet voting system, West Virginia stated, “Future program considerations will require an evaluation of these concerns and the potential costs of additional security measures, if warranted.”⁸⁴

Section 2: United States Projects

The Secretary of State of West Virginia recommended a study committee composed of state, county, and local staff, as well as Internet security experts, to review the “many factors involved in the conduct of this pilot, including voter participating and feedback, security considerations, cost-per-voter, legislative mandates and administrative requirements.”⁸⁵ Additionally the study will include a review of the different technologies employed by Internet voting system vendors.

Standards Used

In the procurement of the voting system, *the Program Element Confirmation Checklist* specifies: accessibility, secret-but-verifiable ballots, data security, and technology specifications.⁸⁶

Level of Risk Assumed

West Virginia required multiple servers from both vendors in an effort to minimize risk of the Internet voting system going offline.

Entity Assuming Risk

The June 9, 2010 *Legislative Report* notes that in regard to the UOCAVA program, “the Secretary of State’s office moved into its capacity as the oversight body responsible for ensuring the pilot was conducted in accordance with the law.”⁸⁷

Voting Over the Internet (VOI)

Sponsor:	FVAP; South Carolina (Statewide); Okaloosa County, FL; Orange County, FL; Dallas County, TX; Weber County, UT
Election Type:	General Election
Date or Voting Period:	September - November 2000
Target Population:	UOCAVA voters
Channel:	Uncontrolled>Vote Data Return>Web Application
Technology Provider:	U.S. Department of Defense (DoD) FVAP
Channel Protection:	VPN between central server and servers at state/county offices; SSL between voters and central server; session and object encryption
Participating Voters:	84
Authentication:	Two factor: User name and password with hard token DoD PKI medium assurance (X.509) digital certificate

Section 2: United States Projects

The Voting Over the Internet (VOI) project was a small project implemented cooperatively by the Federal Voting Assistance Program (FVAP), South Carolina (Statewide); Okaloosa County, FL; Orange County, FL; Dallas County, TX; Weber County, UT. The pilot project was designed to examine the feasibility of using the Internet for remote registration and voting in an effort to overcome the time and distance barriers faced by UOCAVA voters. “This was the first time that binding votes were cast over the Internet for federal, state, and local offices, including the President and Members of Congress.”⁸⁸

The VOI architecture was composed of three segments: the central server site administered by FVAP, the local election office (LEO) server sites administered by the county election offices and the South Carolina State Board of Elections, and the computers used by the voters. A system architecture diagram is located in Appendix G. All system communications took place over the Internet. External communications connections were configured so that voters could only connect to the central server, and only the central server could communicate with the LEO servers. An Intrusion Detection System on the central server monitored all traffic.

The central server site, administered by FVAP, was the focal point for all system services. It included a server, operating system, database management software, application server software, and the VOI custom-developed software. From a functional perspective, the central server identified and authenticated users, allowed users to transfer Electronic Federal Post Card Applications (EFPCAs) and electronic ballots to and from the LEO servers, and performed a “postmarking” function of time-stamping all transactions. The content of all transactions passed through the central server in encrypted form; only the addressing information could be read for message routing.

The central server provided these functions: authenticated voters and objects; transmitted blank EFPCAs to voters; received completed EFPCAs from voters and forwarded them to LEOs; received blank ballots from LEOs and forwarded them to voters; received voted ballots and forwarded them to LEOs; received and forwarded status messages to voters; maintained transaction and security audit logs; and archived data.⁸⁹

One of the challenges faced by the project was finding an efficient and reliable method for converting ballot data from the native formats of the various Election Management Systems (EMS) and other applications (e.g., Pagemaker) into the format required for electronic transmission and vote capture. The final solution was to develop a software application, called the Electronic Ballot Tool. This tool provided the following functionality: Web interface and step-by-step assistance for the creation of electronic ballots, including defining races, candidates, questions, oaths and instructions; dual language capability for those jurisdictions required to provide ballots in languages other than English; and preparation of final electronic ballot files for transmission to the LEO

Section 2: United States Projects

workstation. LEOs copied the completed ballot files to a floppy disk to upload to the LEO VOI server. The ballot tool server did not retain ballot files.⁹⁰ Each LEO site had a server that connected only to the central server to transmit and receive EFPCAs, electronic ballots and voter status messages. The server utilized a database of voter information and ballot assignment information to match each voter with the correct ballot style. Each server stored completed EFPCAs, blank electronic ballots, and voted electronic ballots for its county. The South Carolina server was operated by the State Board of Elections and contained information for all the counties in the state. After the close of the voting period, the LEO servers supported ballot reconciliation and ballot processing. The LEO server could authenticate objects; maintain transaction and security logs; print records; and archive data.

Ballot reconciliation is a procedure to ensure that only one ballot is counted for each voter. Each LEO had a list of voters requesting to participate in the pilot. If anyone on this list returned a ballot by mail, the ballot was held aside unopened until the end of the voting period. If a voter returned voted ballots by both channels, the electronic ballot was counted and the mail ballot remained unopened. Ballot processing is the procedure whereby the voter's identity is separated from the electronic ballot, and the ballot is decrypted and printed. The LEOs transcribed the votes from the HTML-formatted ballots to ballots that could be tabulated by the local tabulating process.

To use the VOI system, the voter's computer had to run a Microsoft Windows 95/98 operating system, have a connection to the Internet, and have Netscape Navigator browser Version 4.05 or higher installed. Macintosh and UNIX platforms could not be used, nor could Microsoft's Internet Explorer browser. Custom software to enable VOI-specific functions, in the form of a browser "plug-in", was provided on a CD-ROM sent to each voter. The CD-ROM contained the required version of the Netscape Navigator browser for voters who needed to upgrade their software to be compatible. The voter needed to have a DoD PKI digital certificate stored on a floppy disk or pre-loaded in the browser.

The voter used their computer to access the VOI central server; request, complete and submit an EFPCA; request, vote and submit an electronic ballot; and make a status request. The LEO server could respond with a number of status conditions such as no EFPCA received, EFPCA denied, EFPCA pending, E-Ballot available, E-Ballot received.

The voter took the following actions to use the VOI system:

- 1) Notify their LEO that they wanted to volunteer for the project.
- 2) Obtain a digital certificate.
- 3) Receive the VOI software and install it on their computer.⁹¹

After completing these activities the voter could logon to the system as follows:

Section 2: United States Projects

- 1) Insert the floppy disk with digital certificate into disk drive.
- 2) Start Netscape Communicator.
- 3) Enter the URL provided by FVAP.
- 4) Enter the certificate password at the login screen.⁹²

Each voter completed and submitted an EFPCA so the LEO had current voter information to assign the appropriate ballot style. When the form was completed, the voter received a blank Affirmation Statement. The voter entered their certificate password again to digitally 'sign' the form before transmitting it to the LEO. In addition to being a voter registration application and absentee ballot request, this activity enrolled the voter on the system access list.

After the LEO approved the EFPCA and the voting period began, the voter requested a blank ballot using the same login process described above. When the LEO received this request, they transmitted a ballot to the voter. The voter recorded their selections online and reviewed their choices on a confirmation screen. An affirmation screen appeared for the voter to enter their digital signature password, and then click on the Electronically Sign and Send button to transmit the voted ballot to the LEO. The voter received notification that the LEO successfully received the E-Ballot.

FVAP required all system users, including voters and LEOS, to obtain DoD PKI medium assurance X.509 digital certificates, to enable the system to identify and authenticate users with a high degree of certainty. The issuing procedure for these certificates required the recipient to appear in person before an issuing authority or a trusted agent and present government-issued photo identification. After receiving and signing the certificate document, the recipient had to access the PKI website, download their certificate to a floppy disk and assign a password. The materials sent to the voter are located in Appendix H.

Standards Used

The VOI pilot system went through two certification processes -- one prescribed by the Department of Defense for information systems and the other prescribed by the State of Florida for voting systems. The two certifications were combined into a single testing campaign. The DoD Information Technology Security Certification and Accreditation Process (DITSCAP) is a structured testing process to validate a system's functional and security features. It provides a comprehensive approach to characterize the anticipated threat scenario and the type and criticality of the system so appropriate testing procedures and standards can be applied.⁹³

The State of Florida requires voting systems to be tested against the Florida Voting System Standards and certified by the State Division of Elections. Other participating states used the National Association of State Election Directors (NASSED) voting system accreditation process based on the 1990 Federal Election

Section 2: United States Projects

Commission Voting System Standards. Both of these standards were used as sources of testing requirements for system functionality and some aspects of system security. However, neither included security standards for Internet technology. The Federal Information Processing Standards (FIPS) and other sources were used to develop testing requirements for the security elements of the system.

The project team spent considerable time and effort reviewing, revising and adapting testing requirements and procedures from these sources, first with the DITSCAP testing group and then with the Florida certification experts. This required analyzing each testing standard or procedure to determine if it could be directly applied to the VOI system. In those instances where there was not a close fit, the intent of the standard or procedure was considered and the wording modified to meet the intent. For example, it was determined that the Florida design, construction and maintenance standards for durable and reliable voting equipment were satisfied because the system used all COTS equipment. In many instances the voting system standards did not apply because they were intended for other types of voting technology. For example, card stock specifications were not applicable because they were intended for paper ballots while the VOI system used electronic ballots.⁹⁴

Level of Risk Assumed

The DoD Information Technology Security System Class analysis performed by the independent testing organization rated the System Class level of the VOI system at 30 out of a possible 47 points. This rating was based on evaluation of the following factors: interfacing mode (Benign), processing mode (System High), attribution mode (Comprehensive), mission-reliance factor (Total), accessibility factor (As Soon As Possible), accuracy factor (Exact), and information categories (Sensitive but Unclassified). The significance of this rating is that it indicates the level of analysis required for system certification. VOI was classed as requiring Level 3, Detailed Analysis.⁹⁵

Recognizing the risks inherent in the system development process, FVAP and the states requested pilot voters to also submit a ballot by mail as a back-up measure. This would prevent an unexpected system outage or other malfunction from disenfranchising any voters. Fifteen voters submitted only E-Ballots. Seven of the 69 mail ballots received arrived after Election Day.

The participating states set a limit of 50 participants per jurisdiction to minimize the risk to any single election.⁹⁶

White hat penetration testing was performed as part of the system certification testing process. Random penetration testing was performed as a system security validation strategy while the system was in operation.

Entity Assuming Risk

FVAP signed Memoranda of Agreement (MOAs) with all the participating states and counties describing the roles and responsibilities of the parties.⁹⁷ FVAP was the program manager and proponent. During the development phase FVAP was responsible for funding; defining functional requirements; establishing standards for security, operations and public information; approving the test plan; conducting system acceptance testing; and obtaining system certification. Pilot jurisdictions assisted in developing functional requirements and identifying potential voters; and pilot procedures; provided personnel to operate their portion of the system; provided space, power, connectivity and security for the system; participated in functional testing; and pursued electronic voting and digital signature legislation, where needed to authorize the pilot in their jurisdiction.

During the operational phase, FVAP was responsible for managing the overall system; administering operating the central server site; providing a help desk for voters and LEOs; collecting performance data; and assessing system performance. States and counties were responsible for performing the LEO election process functions; administering the LEO server sites; collecting and reporting performance data; and working with FVAP to assess system performance.⁹⁸

Through the mechanism of these MOAs, FVAP and the participating states and counties agreed to mutually undertake this project and accept the associated risks.

Section 3 European Projects

Austria

Sponsor:	Federation of Students
Election Type:	Student Union Election
Date or Voting Period:	May 18-22, 2009
Target Population:	Austrian Student Union
Channel:	Uncontrolled>Vote Data Return>Web Application
Technology Provider:	Austrian Federal Computing Center, Scytl ⁹⁹
Channel Protection:	SSL and standard cryptographic methods provided via Java applet
Participating Voters:	2,161
Authentication:	Two-factor: PIN and National ID Card

Austria used an Internet voting system for the 2009 Federation of Students' Student Union election.¹⁰⁰ Three non-legally binding elections (2003, 2004 and 2006) were held prior to the 2009 election to test the voting platform.¹⁰¹ Austrian constitutional law does not allow for the use of Internet voting in Parliamentary Elections. Elections for representation of certain social groups (e.g., Student Union) are regulated by law. The Student Union law was amended in 2001 to specifically regulate Internet voting.¹⁰² These amendments allowed for the 2009 Federation of Students election to be considered a legally binding election. The Federal Ministry for Science and Research administered the project and released an analysis of the project in German.¹⁰³

The Internet voting system was composed of two elements: the electoral administration system and the vote casting system. Scytl was selected as a technology provider to provide the voting system and programmed a portion of the electoral administration system. A major component of the electoral administration system and the vote casting system was the National ID card, which was distributed before the election began.¹⁰⁴ The card was activated through an in-person registration process which verified the identity of the voter. During the process, the voter entered two distinct (four- and six-digit) PINs for use with the card.¹⁰⁵ The card was used at several points during the voting process.

To begin the voting process, the voter navigated to the correct URL. The voter identified and authenticated themselves to the system by inserting their ID card

Section 3: European Projects

and entering both PIN numbers.¹⁰⁶ The voter selected their candidate choices and confirmed the ballot with the six-digit PIN. The PIN is a string known only to that voter. The steps taken by a voter to cast a ballot were:

- 1) Navigate to the correct web address
- 2) Select the voter's University
- 3) Insert National ID card into card reader
- 4) Input the four- and six-digit PIN codes
- 5) Vote the ballot displayed onscreen
- 6) Review the Confirmation screen
- 7) Enter the six-digit PIN to sign and encrypt the vote
- 8) View and store the verification code¹⁰⁷

A system architecture diagram is located in Appendix I.

Table 3-1 provides a timeline of Internet voting in Austria.

Table 3-1¹⁰⁸ Timeline of Internet Voting in Austria

Date	Action taken
2000	Initial idea regarding Internet voting for the Federation of Students
2001	Revision of the Student Union Law to allow for Internet voting
2004	Ministry of Interior establishes an Inter-departmental Working Group
2007	Project started by the Minister of Science
December 3, 2008	Austrian Federal Computing Center and Scytl present the project to the public
March 2009	Certification of voting software
May 18 – 22, 2009	Internet voting available for the Student Union Election
May 26 – 28, 2009	Traditional paper based voting occurs

Standards Used

Austria used the Council of Europe's *Legal, Operational, and Technical Standard for E-voting* to evaluate and certify their Internet voting system. This standard was used as a baseline for the project, with additional requirements created by Austria's Parliament. Common Criteria ISO/IEC 15408 was also used in the system's implementation.¹⁰⁹

Design principles for the system are identified in Robert Krimmer's PowerPoint presentation *Implementing Electronic Voting: The Austrian Experience*:

Section 3: European Projects

- Unequivocal identification of the voter
- With absolute anonymity at the point of casting the vote and
- No possibility for the election administration to change votes or to break the anonymity.¹¹⁰

Additionally, the system was audited by A-Sit, an independent Certification Authority appointed by the Federal Ministry of Science and Research. A-Sit reviewed the source code under a nondisclosure agreement. A group of students was also allowed to view the source code during a one-day workshop.¹¹¹

Level of Risk Assumed

The Internet voting system deployed in Austria was designed as an advance voting channel. Voting occurred nearly one week before polling stations opened for traditional paper-based voting. The timing of these events was a risk mitigation procedure, because if attacks occurred, Internet voting results could be nullified as long as the attack was detected before paper-based voting began. This followed a similar approach to postal voting with regard to voter coercion and vote buying. Postal voting was used as the baseline comparison for risk, but the voting system also had to pass a national certification process.¹¹² As part of the national certification process, an evaluation and certification of the software was required 60 days before Election Day to ensure that the Internet voting system's software complied with the standards set by law and functioned as designed.¹¹³

Entity Assuming Risk

The Austrian National Parliament accepted the risk for the project by passing legislation allowing for Internet voting. In case of attack on the system, provisions were made for the Election Commission to annul the results from the Internet voting system. If an attack occurred, voters would revert to polling place voting. The Election Commission certified the system for use in the election. The voting system experienced a Distributed Denial of Service (DDOS) attack three days before the polls were opened.¹¹⁴

Estonia

Sponsor:	National Election Commission
Election Type:	European & National Parliament and Local Election
Date or Voting Period:	See Table 3-2
Target Population:	General Electorate
Channel:	Uncontrolled>Vote Data Return>Web Application
Technology Provider:	Estonian Government, AS Cybernetica ¹¹⁵
Channel Protection:	Two-way SSL authentication ¹¹⁶
Participating Voters:	See Table 3-2
Authentication:	Two-factor: PIN and National ID Card

Estonia is one of the few countries continuously using an Internet voting system. Polling place and postal voting channels are also offered. The Estonian Internet voting system was developed for, and first used in, the 2005 Local Elections.¹¹⁷ The first binding election occurred in October 2005 and with the success of the 2005 Local Elections, Internet voting was extended to the 2007 National Parliament Elections.¹¹⁸ In 2009, the system use was extended to European Parliament Elections and Local Elections.¹¹⁹ Table 3-2 shows I-voting turnout for Estonian elections.

Table 3-2¹²⁰ Voter Turnout in Estonia

Election	Type	I-Votes Cast	Percentage of Total Votes Cast
2005	Local Election	9,317	1.9%
2007	Parliament Election	30,275	5.5%
2009	European Parliament	58,669	14.7%
2009	Local Election	104,413	15.8%
2011	Parliament Election	140,846	24%

The Estonian government provides all citizens aged fifteen years and above with a National ID card containing a digital certificate.¹²¹ The National ID is considered a key piece of the Estonian Internet voting system because of the high level of authentication it provides to system users. The National ID contains a personal data file, a digital certificate for authentication, and a digital certificate for digital signatures.¹²² The voting system requires voters to provide an Estonian National

ID with the correct PIN codes.¹²³ A smart card reader is used to interface the National ID card with the voter's PC. The *BeVoting Study of Electronic Voting Systems* discusses the steps a voter must take to cast a ballot:

- 1) The voter inserts the ID-card into card reader and opens the webpage for voting (<http://www.valimised.ee>).
- 2) The voter verifies him/herself using the PIN1 of ID-card.
- 3) The server checks if the voter is eligible (using the data from population register).
- 4) The voter is shown the candidate list of the appropriate electoral district.
- 5) The voter makes his/her voting decision, which is encrypted.
- 6) The voter confirms his/her choice with a digital signature (by entering the PIN2-code).
- 7) At the vote count the voter's digital signature is removed and at the final stage the members of the National Electoral Committee can collegially open the anonymous eVotes and count them.¹²⁴

The Internet voting system uses the double envelope scheme, analogous to the way many countries perform postal voting. When a voter makes ballot selections, the voting system encrypts those choices. After encryption of the voter's ballot selections, the vote is digitally signed before transmission.¹²⁵ Upon receiving the encrypted vote, the National Election Commission validates the digital signature, removes it, and stores the now anonymous voter selections in an electronic ballot box for later tabulation.¹²⁶ A system architecture diagram is located in Appendix J.

Standards Used

The National Electoral Committee of Estonia commissioned a working group which produced a report titled *E-Voting conception security: analysis and measures* in 2003. This analysis addressed "the issue of security risks in the technical conception of e-voting proposed by the National Electoral Committee."¹²⁷ The document describes high level requirements for properties such as: auditability, secrecy, error protection, security, and unprovability. Over fifty high-level requirements are detailed and recommended in the document.¹²⁸

The National Electoral Committee recommended "the general security of the system be based on Information Systems Three-level security model for information systems (ISKE) High security class."¹²⁹ The Council of Europe's *Legal, Operational, and Technical Standard for E-voting* was also used in the system's development.¹³⁰

Level of Risk Assumed

The *E-Voting conceptions security: analysis and measures* report contains a security analysis and a list of protection measures against major risks. A list of

Section 3: European Projects

specific risks accepted by the Estonian National Electoral Committee is summarized below:

- Need to spend resources on organizational and technical security
- Need to trust voter's computer and public network
- Need to trust Central System computers
- Impossibility to support all voters
- Concentration of risks and the possibility of negative media report
- Risks deriving from formalization of processes¹³¹

The report finds:

We believe that the risks of the described voting scheme can be managed so that the possibility of the dangers becoming a reality or the damage caused is acceptably small. It can be said that by putting different parts of the system to distrust and monitor each other and adding control by humans where necessary, we achieve sufficiently secure e-voting system.

Naturally organizational measures, i.e. division of tasks and responsibility, formal procedures, awareness and managing of risks by NEC, prepared action plans for solving emergency situations, independent audit, have to be added in accordance with the technical measures (cryptography, intrusion detection, double control of data, etc.).

We believe that on the basis of the conception offered by us it is possible to create an e-voting mechanism whose security is higher than that of conventional voting with ballot papers. This requires well-planned technical solution, careful development work and – what is the most important – responsible use, but all systems that are as critical require that.¹³²

Entity Assuming Risk

The *E-Voting conceptions security: analysis and measures* document did not include an analysis on the body of government assuming risk. Since many of the risks highlighted by the National Electoral Committee were labeled as “accepted”, the National Electoral Committee, who designed and operated the system, accepted the risk for the implementation and fielding of the Internet voting system.

Finland

Sponsor:	Ministry of Justice
Election Type:	Municipal Election
Date or Voting Period:	October 26, 2008
Target Population:	Registered voters of Kauniainen, Karkkila and Vihti
Channel:	Controlled>Vote Data Return>DRE/Kiosk
Technology Provider:	TietoEnator, ScytI
Channel Protection:	VPN ¹³³
Participating Voters:	12,234 ¹³⁴
Authentication:	One-factor: Proof of identity via an official photograph presented to election official

On October 26, 2008, Finland conducted Municipal Elections piloting an Internet voting system. Three municipalities (Kauniainen, Karkkila and Vihti) allowed voters the choice between traditional voting methods or electronic voting machines connected to the Internet in the polling place. These were the first elections in Finland to use Internet voting as a viable voting channel. Table 3-3 provides the total Election Day turnout.

Table 3-3¹³⁵ Voter Turnout in Finland

Jurisdiction	Turnout (traditional voting methods)
Kauniainen	2,165
Karkkila	2,982
Vihti	7,087

The kiosk machines provided for controlled Internet voting at a polling place.¹³⁶ The voter used the voting application on the kiosk to make ballot selections, which were then transmitted to a central server via the Internet.¹³⁷ Votes were encrypted and digitally signed within the voting kiosk before transmission via the Internet.¹³⁸ A mixing application was used at the central server to shuffle the votes and make the ballots anonymous prior to tabulation.¹³⁹

To cast a vote electronically a voter:

- 1) Provided an election official with a document with a photo of the voter
- 2) Received a voting card
- 3) Inserted the voting card into the electronic voting kiosk

Section 3: European Projects

- 4) Followed the instructions on the screen to make ballot selections
- 5) Removed the voting card from the machine
- 6) Provided the voting card to an election official¹⁴⁰

Based on a report issued by the Finnish Ministry of Justice, if the voter “removed the voting card from the card reader before confirming the choice by pressing the OK button” the cast ballot was not registered.¹⁴¹ This issue impacted 232 voters on Election Day and required new elections, held in September 2009, for the municipalities that used the e-voting pilots.¹⁴²

In 2010, the Finnish Cabinet decided to maintain the current election system and shelve e-voting for the time being.¹⁴³ Another e-voting pilot will not be considered for the 2016 municipal elections.¹⁴⁴

Standards Used

The regulations for elections in Finland are outlined in the Constitution of Finland, the Election Act (714/1998) and provisions included in the Act which amended the Election Act (880/2006).¹⁴⁵ The Finnish government used a variety of standards and “put significant resources into ensuring that the electronic voting would be carried out in line with national legislation and international standards, including Recommendation (2004)11 of the Committee of Ministers of the Council of Europe.”¹⁴⁶

The Internet voting system’s source code and design was reviewed by experts from the University of Turku. A report with the results of the expert analysis was published and used as part of the certification process.¹⁴⁷

Level of Risk Assumed

The Finnish Ministry of Justice’s website states:

Considering the central principals of holding elections in Finland it is important that voting takes place in front of election authorities. This is why electronic voting is possible only at the advance polling stations and the polling stations on Election Day.

In Internet voting (distance voting), taking place at home or at work, it would not be possible to ensure that every voter has an equal voting right and a secret and free election. It would be impossible to ensure that no one sees who the voter votes for. Voting could turn into “family voting,” where the head of the family decides who the family vote for.

Some of those entitled to vote are not interested in elections or voting. This could lead to a situation where a person chooses to surrender his or her right to vote to someone else. Also selling votes might become a problem.¹⁴⁸

The Ministry of Justice stated a number of questions relating to the implementation of Internet voting that “no good answers” exist for:

- How can the election secrecy of the voter be ensured, if someone else is able to see who he or she votes for?
- How can free elections be ensured, if someone else may be able to force the voter to vote in a certain way?
- How can the equal right to vote be ensured, if the voter may surrender his or her right to vote to someone else, for instance, because he or she is not interested in the election?
- How can selling and buying votes be prevented?
- How can the principle of equal treatment be achieved, if it cannot be ensured that everyone has access to the necessary technical equipment or know how to use it? Would it be fair that young people could vote at home and older people would have to go to the polling station?¹⁴⁹

Entity Assuming Risk

The Ministry of Justice assumed the risk for the e-voting pilot.

France

Sponsor:	Ministry of Foreign Affairs and Local Officials
Election Type:	See Table 3-4
Date or Voting Period:	See Table 3-4
Target Population:	Varies by Pilot
Channel:	Controlled and Uncontrolled forms of Internet voting
Technology Provider:	The EAC was unable to obtain this information
Channel Protection:	The EAC was unable to obtain this information
Participating Voters:	The EAC was unable to obtain this information for some of the pilots (see below)
Authentication:	The EAC was unable to obtain this information

The EAC was able to locate information for six French Internet voting pilots but was unsuccessful in obtaining detailed information on many of the specifics of the pilot projects. The EAC obtained enough information to discuss the projects at a high-level.

Section 3: European Projects

In 2001, Voisins-le-Bretonneux conducted an Internet voting pilot using a kiosk in the polling station for the municipal elections.¹⁵⁰ Another pilot took place in Vandoeuvre-les-Nancy providing network voting in polling stations for the Presidential election in April and May 2002. In June 2002 they experimented with the use of smart cards containing voter's fingerprints for the legislative elections. In November 2002 Issy-les-Moulineaux tested a pilot during a local council election using Internet voting. About 1449 people elected to participate, 939 received the secret code and of those, 860 used the Internet option.¹⁵¹

In May 2003, French citizens residing in the U.S. were given the possibility to use remote Internet voting to elect their representatives to the Assembly of the French Citizens Abroad (AFE) (previously the Conseil Supérieur des Français d'étranger (CSFE)). About 8% of the 61,056 registered voters in the U.S. cast their vote over the Internet.¹⁵² In 2006, this method was again available, and was offered to citizens living abroad in any country.¹⁵³

In 2009, the French Ministry of Foreign Affairs implemented an Internet voting platform for French citizens living overseas.¹⁵⁴ This allowed 310,000 French voters in Africa and the Americas to vote for their representatives to the AFE.¹⁵⁵ The Internet voting platform was available 24 hours a day until polling place voting opened on June 7, 2009.¹⁵⁶ This initiative was designed to address the obstacles overseas citizens face with the current voting process and to increase participation among overseas voters.¹⁵⁷ ScytI, in partnership with Atos Origin, was the technology provider for the secure voting platform.¹⁵⁸ The technology was reviewed, certified and a risk assessment was conducted by the Ministry of Foreign Affairs through an audit provided by Opida, an independent security consulting company.¹⁵⁹

Table 3-4 provides a timeline of the Internet voting projects performed in France.

Table 3-4 Timeline of Internet voting in France

Year	Election Type	Location
2001	Municipal	Voisins-le-Bretonneux
2002	Presidential	Vandoeuvre-les-Nancy
2002	Local Council	Issy-les-Moulineaux
2003	AFE	French voters residing in U.S.
2006	AFE	French voters residing abroad
2009	AFE	French voters residing in the Americas or Africa

Section 3: European Projects

In June 2006, the Association Démocratique des Français de l'Étranger – Français du Monde asked François Pellegrini to conduct an evaluation of the Internet voting system in use since 2003.¹⁶⁰ The report outlined these concerns:

- The secrecy of the vote could be violated due to the small number of people voting over the Internet and the fact that the Chairperson and each Voting Office received a list of the voters (by method) and the total votes cast for each candidate.
- The system use third party libraries and the source code were not available if corrections or alterations in the program were necessary.
- The hardware was considered proprietary and not available for verification.
- Internet voting is subject to results being destroyed or falsified by a small group of individuals in various ways, including: denial of service attacks, DNS (Domain Name System) poisoning or viruses.
- The system did not produce hardcopies of data or information.¹⁶¹

Standards Used

The National Commission for Information Technology and Liberty (CNIL) provided guidelines related to e-voting security which was used by CNIL and Opida to certify the security of the Scytl voting platform.¹⁶² Additionally, Opida incorporated security standards from the National Agency of Information Technology Security (ANSSI) for their audit.¹⁶³

In July 2003, CNIL adopted a set of recommendations regarding Internet voting:

- Separation of data relating to the name of the voter from the votes file in distinct IT and encryption of the electronic vote.
- Make it impossible for staff managing or maintaining the IT system to access information concerning the counting of votes, which should be encrypted with encryption keys and the decryption information conserved in a sealed form.
- Remote servicing should be forbidden during the counting of votes until the end of the appeals period.
- Access to the software's source code and use of public encryption algorithms should be available.
- The system should provide a complete trace of its internal operations to provide a solid basis for external audits and should ensure effective monitoring of electoral processes.
- The servers and other central IT resources should be located in national territory.
- There should be public verification of the initial state of the system before counting votes.¹⁶⁴

Section 3: European Projects

The Forum des Droits sur l'Internet (Internet Rights Forum), a private non-profit association, whose members are comprised of “public bodies, associations and companies,” was set up by the French government in May 2001.¹⁶⁵ In September 2003, the Forum published a report, *Quel Avenir pour le Vote Electronique en France?* which included these recommendations:

- Remote electronic voting should only be used for residents abroad; electronic voting machines in polling places are recommended.
- There should be absolute separation of the IT management of electoral records and electoral ballot boxes. Access by nominated experts to the source code.
- Audits of the voting system after each election.
- Voting servers must be located in French territory.
- Remote electronic voting should be available for several days and completed prior to Election Day. The voter should be able to alter their vote up to final validation.
- An electronic voting observatory should be created to centralize information and lessons learned from electronic voting experiments, including voting experiments abroad.¹⁶⁶

Level of Risk Assumed

The mitigations instituted for the 2009 election were:

- Source Code Review: Opida and external observers were allowed to review the source code.
- Certification: Opida, Ministry representatives, and external observers certified the source code and participated in the compilation and digital signature of the binaries generated.
- Continuous audit process: Opida and Ministry representatives performed random audits of the voting platform components before, during and after the election.
- End-to-end encryption: Votes were encrypted and digitally signed in the voting terminal before they were sent to the voting servers.
- Mixing protocol: Any correlation between voting order and votes was broken using a cryptographic mixing, shuffling and decryption scheme.
- Voter verifiability: Voters can verify the presence of their votes using cryptographic voting receipts that do not disclose voter intent.¹⁶⁷

Entity Assuming Risk

The Ministry of Foreign Affairs assumed the risk for the pilot projects.

Netherlands

Sponsor:	Ministry of the Interior and Kingdom Relations
Election Type:	Federal Election, European Parliament
Date or Voting Period:	2004: June 1-10, 2004 2006: November 18-22, 2006
Target Population:	Dutch voters living abroad ¹⁶⁸
Channel:	Uncontrolled>Vote Data>Web Application
Technology Provider:	LogicaCMG and Rijnland District Water Control Board
Channel Protection:	The EAC was unable to obtain this information
Participating Voters:	2004: 480 telephone, 4871 internet ¹⁶⁹ ; 2006: 19,815 ¹⁷⁰
Authentication:	One-factor: Voter Code

In 2000, the Ministry of the Interior and Kingdom Relations began a remote e-voting project. The goals of the project were to increase voter turnout and to make the voting process less location dependent in the Netherlands and abroad.¹⁷¹

In 2004, Dutch citizens living and working abroad were able to vote in the Parliamentary Elections via telephone and the Internet. LogicaCMG was contracted as the supplier of these two voting channels. At the same time, Rijnland District Water Control Board (Rijnland) was developing an Internet voting system, called the Rijnland Internet Election System (RIES) for their own water board elections. The Ministry of the Interior and Kingdom Relations and Rijnland decided to cooperate together and exchange experiences and knowledge. The Ministry decided to use the RIES system for the Dutch voters abroad in 2006 during the European Parliament elections because:

1. The voters had the option to check for themselves if their vote has been received well and counted.
2. RIES was successfully used in a large pilot project
3. The wish to conduct this pilot project with another governmental institution.¹⁷²

The RIES system gained the EU's 2005 eGovernment Good Practice Label and the UN's 2006 Public Service Award. At the time of publication, source code, documentation, and a demonstration of the RIES Internet voting system can be viewed at <http://www.openries.nl/>.¹⁷³

In the Netherlands voters who reside in the country do not register to vote; however, Dutch citizens who live abroad or are on the day of the election abroad for their work have to register themselves via postal mail.¹⁷⁴ International media

Section 3: European Projects

and embassies were among the channels which were used to promote voter registration for Dutch voters living abroad.¹⁷⁵ In 2004, the voter could cast a vote via telephone, Internet, postal mail, or at a polling station on Election Day. In 2006, voters could chose to vote from all of the channels provided in 2004, except the telephone.

In 2004, voters, when registering, also registered a personal, five digit code.¹⁷⁶ After registration, the voters received another code and voters accessed the online ballot by using both codes.¹⁷⁷ In 2006, voters did not register their own personal code, because they sometimes had problems remembering their code. Therefore, in 2006, the voters received a voting card, which held a voting code (a cryptographic key) and a brochure on Internet voting.¹⁷⁸ Voters were emailed a list of candidates and an image of the 2004 and 2006 Internet voting card, sent to voters via postal mail, is located in Appendix K.¹⁷⁹

The systems used a JavaScript Internet browser application for the voter to cast the ballot.¹⁸⁰ The voter casts a ballot from their PC by:

- 1) Navigating to the correct web address
- 2) Entering the voting code (in 2004 also entering the voter's personal code)
- 3) Making ballot selections
- 4) Casting the ballot to election server
- 5) Receiving a receipt confirmation¹⁸¹

The receipt confirmation, also known as a technical vote, allows voters to verify their vote was counted.¹⁸² The information initially sent to the voter instructed them to destroy their voting code confirmation after use. If a voter publicizes their voting code and receipt confirmation; their vote can be confirmed by an outside party by trying all possible voting codes and receipt confirmations.¹⁸³ The RIES system required the list of voting codes to be kept safe from disclosure before the election began and the codes were destroyed after the election ended. The *2006 OSCE/ODIHR Election Assessment Mission Report* states:

“The designers of RIES have effectively opted to surrender protection against coercion of a voter in favour [*sic*] of greater transparency. It is important to note that this feature is inherent in many Internet voting systems and in most postal voting, where voters can surrender secrecy by simply allowing observation of their actions whilst voting.”¹⁸⁴

Standards Used

The RIES system was originally not developed to a formal set of standards.¹⁸⁵ During the process of adjusting the system for the 2006 elections, the Council of Europe's *Legal, Operational, and Technical Standard for E-voting* was incorporated.¹⁸⁶

Level of Risk Assumed

A former Dutch Federal election employee stated:

Since Dutch voters living or working abroad already had the option of voting via post, voting via telephone did not entail new risks. With regard to the telephone voting, the eavesdropping threat was identified and resolved by sending voters a customized ballot paper with each candidate having a unique code, so that if eavesdropping occurred, it could not be determined what the content of the vote was.

With regard to the Internet voting, the general risks were identified and, consequently, tests were conducted, including: acceptance testing, performance testing, stress testing, security testing, review of the source code, testing of functional design, testing of safeguards, scenario testing, browser testing, technical testing, penetration testing, security scan and analysis and a small pilot to also test the usability.¹⁸⁷

Entity Assuming Risk

The Ministry of the Interior and Kingdom Relations was responsible for the system.

Norway

Sponsor:	Ministry of Local Government and Regional Development
Election Type:	Federal Election
Date or Voting Period:	August 10 – September 12, 2011
Target Population:	General Electorate
Channel:	Uncontrolled>Vote Data Return>Web Application
Technology Provider:	Norwegian Government, ScytI, ErgoGroup
Channel Protection:	HTTPS ¹⁸⁸
Participating Voters:	0
Authentication:	One-factor: Username/password ¹⁸⁹

In 2004, the Norwegian Ministry of Local Government and Regional Development appointed a Working Committee to assess “the potential and possibilities of introducing e-voting in Norwegian elections and, if recommend, to assess how such a system can be implemented.”¹⁹⁰ In February 2006, the *Electronic voting – challenges and opportunities* report was released by the Working Committee. The report analyzed whether introducing voting

technologies (e.g., postal voting, touch screens, SMS voting, digital TV, and Internet voting) is feasible, economically and technologically, and how these technologies could be implemented.¹⁹¹ The Working Committee presented an approach for introducing different types of e-voting pilots in controlled (e.g., polling place) and uncontrolled environments (e.g., Internet voting).¹⁹² An important conclusion from their report is:

An absolute requirement for e-voting in uncontrolled environments is that the system builds on very strict security requirements and that the methods developed do not reduce the voters' confidence in the system. Current technology cannot guarantee this. The working committee is therefore of the opinion that e-voting is not at present recommendable on a large-scale basis.¹⁹³

In 2009, the Ministry of Local Government and Regional Development announced a limited Internet voting system trial.¹⁹⁴ The system will be piloted in ten Norwegian municipalities for the 2011 local and county elections, during advance voting only, from August 10 – September 12, 2011. Information from this pilot will be used for the Norwegian Parliament to make a decision about future, large scale implementation.¹⁹⁵ The Internet voting system's technical documentation and source code is publically available.¹⁹⁶ The Ministry posted multiple academic reviews and studies of the cryptographic protocols used by the system on their website.¹⁹⁷

The system design is similar to the "double envelope method" used in postal voting. The use of receipt codes is an added feature "to detect when a compromised computer has altered the ballot."¹⁹⁸ The receipt codes are provided to the voter through a different electronic channel, such as a cell phone. The voter can then verify the receipt codes received from the cell phone against a list of codes already computed and printed on the voter card initially sent to them.¹⁹⁹

Standards Used

The 2004 Working Committee recommended using the Council of Europe's *Legal, Operational, and Technical Standard for E-voting* standard if implementing e-voting is to occur on a large scale. Also, the committee proposed a number of general requirements for system architecture and noted a need for detailed requirements and specifications for e-voting systems.

The award for the system was issued in 2009 for system implementation in 2011. The *Final tender document* contains award criteria based on cost, implementation methodology, and proposed solution.²⁰⁰ The *specification, tenders, evaluation and contract* website provides over fifty documents describing the system. The *System Requirements Specification* document provides a large amount of requirements and echoes the need for the Council of

Section 3: European Projects

Europe's Recommendation, stating: "In case of conflict between the Recommendation and the System Requirements Specification, the latter has priority)."²⁰¹

High-level security objectives are documented in the *e-Vote 2011 Security Objectives* document:

- Vote Authenticity
- Voter Anonymity
- Data Confidentiality
- Data Integrity
- System Accountability
- System Integrity
- System Disclosability/Openness
- System Availability
- System Reliability
- Personnel Integrity
- Operator Authentication and Control²⁰²

Level of Risk Assumed

Risk is addressed in detail in the *e-Vote 2011 Security Objectives* document.²⁰³ The document is based on the *e-Voting Security Study, Issue 1.2*, from the UK's National Technical Authority for Information Assurance. The risk management strategy stated in the document is:

Despite the attempts to secure the system, it is probably impossible to make any system perfect at reasonable cost. This leads to the conclusion that a sensible risk management-based approach needs to be established.

The Contractor will therefore be required to keep a continuously updated threat model enumerating the identified threats, vulnerabilities and corresponding mitigations, as well as a risk assessment of his/her deliverables including required security in the operating environment of the deliverables.

The key questions to be answered by the Contractor are what is the remaining risk given the application of security mechanisms and why should the remaining risk be acceptable to e-vote 2011 project?²⁰⁴

The document includes assumptions made while developing the system and threats to the voting system²⁰⁵.

Entity Assuming Risk

The Ministry of Local Government & Regional Development assumed the risk for the system.

Portugal

Sponsor:	Portuguese Parliament and Government
Election Type:	Portuguese Parliamentary Election
Date or Voting Period:	February 2005
Target Population:	Portuguese citizens residing abroad
Channel:	Uncontrolled>Vote Data Return>Web Application
Technology Provider:	NOVABASE
Channel Protection:	The EAC was unable to obtain this information
Participating Voters:	4,367 ²⁰⁶
Authentication:	One-factor: Username/password

During the 2005 Parliamentary Elections, a consortium led by the Knowledge Society Agency - Ministry of Science, Technology and Higher Education (UMIC), conducted Portugal's first pilot of Internet voting for Portuguese citizens residing abroad. About 150,000 registered citizens living abroad received two mailings: one with the paper ballot and one with instructions and codes for using the Internet system.²⁰⁷ Voters were required to vote the paper ballot for the official record and given the option of testing the Internet voting method.

The Internet voting process was:

- 1) A unique username and password were generated for each registered overseas voter who requested a paper ballot.
- 2) Voter information and the unique credentials were registered in the Active Directory of the central system.
- 3) Officials sent the credentials to overseas voters via postal mail. This mailing did not include the elector number, as an additional security measure.
- 4) Encryption keys were generated by the system. The public key was stored in the NOVABASE database; the private key was broken into 7 parts, requiring all 7 keys to read votes.
- 5) The voter accessed the website and provided their elector number and the credentials for verification.

Section 3: European Projects

- 6) The voter made selections and confirmed the selections, casting the ballot.
- 7) The confirmed vote was registered in the database table using two key encryption. At the same time, the Active Directory recorded that the voter cast a ballot. Upon completion of this process, the voter received confirmation that their ballot was accepted.
- 8) At the close of voting, the data in the Active Directory was printed and sent to the Comissão Nacional de Eleições (CNE).
- 9) Comissão Nacional de Protecção de Dados (CNPD) officials witnessed the erasure of the Active Directory. CNPD is a unit that oversees the use of personal information in databases. A copy of the database is stored with UMIC.
- 10) The 7 keys were used to gain access to the results. Another application was used for tabulation.²⁰⁸

Standards Used

The EAC was unable to obtain this information.

Level of Risk Assumed

The EAC was unable to obtain this information.

Entity Assuming Risk

Risk was shared among UMIC, CNE, Secretariado Técnico dos Assuntos para o Processo Eleitoral (STAPE), CNPD and the Universidade do Porto. UMIC served as the coordinator for this project.

Spain

Sponsor:	Oficina de Coordinació Electoral, Catalonia
Election Type:	Non-binding Pilot for Election to the Parliament of Catalonia
Date or Voting Period:	November 16, 2003
Target Population:	Catalan Citizens Living Abroad
Channel:	Uncontrolled>Vote Data Return>Web Application
Technology Provider:	Scytl
Channel Protection:	The EAC was unable to obtain this information
Participating Voters:	730 ²⁰⁹
Authentication:	One-factor: 16 character voter identification key

Section 3: European Projects

The Oficina de Coordinació Electoral conducted a non-binding pilot election for the 2003 Election to the Parliament of Catalonia.²¹⁰ The Oficina de Coordinació Electoral chose Scytl's Internet voting platform to conduct the election. Over 23,000 registered voters residing in a variety of countries were invited to participate in this pilot. Any computer with a browser supporting Java was able to cast a vote in this election. Many of the Catalan cultural associations throughout the world allowed voters the opportunity to use computers in their offices.²¹¹

To cast a ballot in the election, a voter received credentials to access the Internet voting system. The process of providing voters with logon credentials was identical to the process traditionally used for elections; credentials were delivered by postal mail.²¹² After a voter supplied their credentials to the voting system, they were allowed to make ballot selections. When the ballot selections were confirmed, they were then encrypted and transmitted over the Internet. The voter received a receipt containing a unique vote identifier and the digital signature of their vote identifier concatenated with other election data to tie the receipt to that election.²¹³

Standards Used

The Catalan Government set specific objectives that were used to judge success of the pilot, stating the Internet voting system must accomplish the following:

- Facilitate the participation of voters residing abroad. At present, these voters can only vote by mail. Many voters do not receive their ballot or have problems sending it back on time, which causes disenfranchisement.
- Guarantee the honesty of the electoral process. The system must offer at least the same level of security and confidence found in traditional paper-based postal voting.
- Facilitate participation in the election. The installation of any specific software or hardware should not be required.
- Extend the polling period without increasing the man-hours required to staff the election. The current postal voting system entails a logistical challenge that new technologies can simplify and make less expensive.
- Protect the voter's personal data from third parties. This security measure is essential to ensure compliance with the Spanish Law of Personal Data Protection.
- Obtain the results immediately after the polls close. This permits the integration of the results from the remote voting with the results from the polling-place voting without having to wait several days for the postal votes to arrive.²¹⁴

Level of Risk Assumed

One goal of the Oficina de Coordinació Electoral was “to evaluate the advantages, usability, security and reliability of this voting system in consideration of its potential use in future elections which would be mainly as a complementary channel to postal voting.”²¹⁵ Additionally, the Pilot Objectives set by the Catalan Government stated: “The system must offer at least the same level of security and confidence found in traditional paper-based postal voting.”²¹⁶ As this was an election with non-binding results, the level of risk was relatively low.

Entity Assuming Risk

The Oficina de Coordinació Electoral, Catalonia, assumed the risk for this non-binding election.

Sweden

Sponsor:	Ministry of Justice
Election Type:	Not used in an Election
Date or Voting Period:	Not scheduled for use in Election
Target Population:	No system implemented
Channel:	No system implemented
Technology Provider:	No system implemented
Channel Protection:	No system implemented
Participating Voters:	No Participating Voters
Authentication:	No system implemented

In 2000, the Swedish Ministry of Justice released an excerpt in English of the *Final Report of the Election Technique Commission*.²¹⁷ This excerpt details the requirements an electronic voting system must meet to be used in Swedish Federal elections. The Election Technique Commission concluded that any electronic voting system must meet these requirements, including Internet voting systems. The report deemed polling-place electronic voting much more feasible than Internet voting.²¹⁸ Consequently, Internet voting has not been used in a binding election in Sweden.

The Election Technique Commission outlined a phased, “multi-stage procedure” to introduce Internet voting:

- 1) Internet voting in the voter’s polling station
- 2) Internet voting in any polling venue whatsoever

Section 3: European Projects

- 3) Internet voting from public computers
- 4) Internet voting from any computer whatsoever²¹⁹

The excerpt provides details on how Internet voting systems could meet each of these requirements and provides discussion on the importance of each stage to the process of introducing and implementing Internet voting.²²⁰

In 2001, the Swedish Federal government supported an Internet voting pilot at Umeå University.²²¹ The pilot was supported by the Federal government because the Election Technique Commission suggested that school election trials are considered “not so risky.”²²² An American company, Safevote Inc., provided the technology for the election and was required to follow the principles outlined in the Final Report of the Election Technique Commission.

Although the implementers viewed the election a success, the Swedish Agency for Public Management and Government Proposition on Democracy concluded in an evaluation report that “security in Internet voting is not yet good enough for general political elections.”²²³ Further information regarding other pilots was not located.

Standards Used

The Election Technique Commission issued these conclusions:

The point of departure is that a system of electronic voting (‘e-voting’) via the Internet must fulfill the following five basic requirements:

- Only people eligible to vote should be able to vote.
- It should be possible to use one’s vote only once.
- Ballots should be absolutely secret.
- It should not be possible for a vote cast to be changed by anyone else.
- The system should ensure correct tallying of votes at all levels (voting district, constituency and area).²²⁴

The Commission presents an e-voting system for Internet (online) voting that should be capable of fulfilling these requirements. Before it is tested in an election, however, extensive trials should be carried out. After the trial, a final decision is made about whether the procedure is applicable in a real election.

Level of Risk Assumed

The *Final Report of the Election Technique Commission* states “...the system must be at least as secure as corresponding traditional voting procedures.”²²⁵ The report also states:

Sweden’s use of a paper-based, mainly manual voting procedure is not due to technical backwardness. Instead, according to Olsson, the reason

is that an IT solution is far too vulnerable in purely physical terms. Saboteurs could cause disruption in telecoms and the power supply. Another reason, according to Olsson, is protection for ballot secrecy, i.e. the need to prevent any outsider from being able to find out how one has voted. This means, too, that certain transactions in a voting system cannot be revised after the event. Otherwise, a guarantee for citizens' confidence in this type of system lies in the fact that the computer programs that make the decisions are public and can be tested with their own data.²²⁶

Entity Assuming Risk

An Internet voting system was not used in a Swedish governmental election.

Switzerland

Three of the 26 Swiss cantons own and operate Internet voting systems: Geneva, Neuchâtel, and Zurich. Each canton offered citizens a choice between three voting methods: traditional polling stations, postal voting and Internet voting.²²⁷ Political rights in Switzerland are addressed at three levels of government: national (federal), cantonal (state), and communal (local/municipal jurisdictions). Each canton is individually responsible for conducting elections on a national, cantonal, or communal level.²²⁸

Geneva, Neuchâtel, and Zurich each employ different systems to serve their voters. Geneva contracted with the State Information Technology Centre, Wisekey and one unidentified company to implement their system, Neuchâtel contracted with ScytI, and Zurich contracted with Unisys. Zurich and Geneva are both working with other Cantons in Switzerland to allow the use of their voting system by the Swiss Abroad (SA) citizens. The SA are Swiss citizens living outside of Switzerland.²²⁹ The SA are required register to vote at an official election office and must review their registration status every four years.

Switzerland's legal framework for Internet voting is unique stating: "upon demand by interested cantons and communes, distant electronic voting can be authorized by the federal government as an additional channel. The federal government may limit/withdraw its authorization."²³⁰ Currently, a maximum of 10% of federal voters are offered remote electronic voting and the legislation allowing this will expire in 2013. The cantons retain the right to offer distant electronic voting if the election is solely comprised of cantonal and/or communal referenda.²³¹ Appendix M provides an account of every Swiss election using an Internet voting system, shown by canton.

Swiss Federal Mandates

The Swiss e-voting initiative was introduced in 2002 with the creation of a legal basis and recommendation as quoted from the Geneva State Council *Report on*

Section 3: European Projects

the electronic vote, Opportunity, risks and feasibility. The Federal Council asserted:

- eVoting should be as easy, practical and safe as possible.
- It should under no circumstances penalize citizens who have no access to electronic communication methods.
- The electorate should be able to express themselves in one and the same poll on federal, cantonal and municipal issues.
- The technical infrastructure should be reliable.
- The system should make it possible to verify voting capacity.
- It should help prevent abuse, facilitate the counting of all votes and protect voting secrecy.²³²

Geneva

Sponsor:	Geneva State Council
Election Type:	Referenda and Initiatives
Date or Voting Period:	See Appendix M
Target Population:	Genevans abroad
Channel:	Uncontrolled>Vote Data Return>Web Application
Technology Provider:	State Information Technology Centre, Wisekey One Unidentified Company
Channel Protection:	SSL with a second layer of encryption provided via Java applet
Participating Voters:	The EAC was unable to obtain this information
Authentication:	Two-factor: PIN from Voter Card and Personal Information

Geneva's Internet voting system was approved by the Geneva State Council in March of 2001.²³³ The government of Geneva states "voting is not something that can be left to the private sector."²³⁴ Therefore, Geneva is the owner and administrator of its system. Geneva's system was developed by the State Information Technology Centre, along "with the collaboration of two private companies chosen by tender."²³⁵

The first step in Geneva's Internet voting process was the voter's receipt of the Voter Card included in Appendix O. The Voter Card contained the information a voter required to cast a ballot via the Internet, postal mail, and polling place voting.²³⁶ To vote via the Internet, the voter used the information on the Voter

Card to identify themselves to the system. The voting system supplied the voter with a statement regarding the penalty for proxy voting, which is forbidden in Switzerland. The voter received an electronic representation of a ballot and then made ballot selections. A confirmation screen containing all of the voter's choices was displayed. The system requested the voter's PIN code, which was hidden on the Voter Card under a scratch off layer of film. After entering the PIN code, the voter submitted the ballot to the voting server. In Geneva, the voter's birthday and municipality of origin is not public information and is used as another authentication mechanism.²³⁷

Standards Used

The Geneva State Council adopted and integrated the security requirements mandated by the Federal Council into their system.²³⁸ These requirements mandated voter privacy as well as auditing of the voting system. Along with meeting the Federal Council's requirements, the Geneva State Council enforced the following 11 requirements for their Internet voting system:

- 1) Votes cannot be intercepted nor modified
- 2) Votes cannot be known before the ballot reading
- 3) Only registered voters will be able to vote
- 4) Each voter will have one and only one vote
- 5) Vote secrecy is guaranteed
- 6) The voting application will resist any DoS attack
- 7) Voters will be protected against identity theft
- 8) Number of cast votes = number of received ballots
- 9) It will be possible to prove that citizen X voted
- 10) The system will not accept votes outside the ballot opening period
- 11) The system will be auditable²³⁹

In addition to the 11 requirements, ISO 27001 and ISO 27002 were used as a basis for Geneva to test their Internet voting system. Due to budgetary restrictions Geneva did not pay for the formal ISO certifications.²⁴⁰

Level of Risk Assumed

The *State Council's Report* included an appendix with an "Inventory of risk and their equivalent in traditional ballots."²⁴¹ The appendix listed many of the risks associated with Internet voting and the corresponding legal basis applicable for each risk. The risk inventory also listed the equivalent risks existing with other Swiss voting channels such as postal and polling place voting.²⁴² The entire inventory of risks can be found in Appendix 1 of the *State Council's Report*.

Geneva determined that "Internet voting must be at least as secure as postal voting."²⁴³ Additionally, Geneva stated there is a "Maximum need for integrity,

Section 3: European Projects

confidentiality, availability and compliance of systems and data.”²⁴⁴ The *Summary of risk assessment* details Geneva’s risk assessment of its own Internet voting system.²⁴⁵ Several assessment methodologies were used, including the State of Geneva’s internally developed methodology for managing the security of information systems. According to the document, there were two risk analysis phases:

- Identification - based on scenarios representing both threats and vulnerabilities, analysis - in terms of probability (P) and impact (I) and evaluation - of risk level (R = PI).
- From selected critical risks, the hardware items involved in the risks scenario are identified and the risk associated with the hardware item is calculated ...²⁴⁶

In the *Report on the electronic vote, Opportunity, risks and feasibility* the Federal Council specifies the level of security of eVoting systems and states “the new system should be...as secure as the current system, which does not mean it should be 100% secure.”²⁴⁷

Entity Assuming Risk

The Canton of Geneva assumed the risk for the voting system.

Neuchâtel

Sponsor:	Canton of Neuchâtel
Election Type:	Referenda and Initiatives
Date or Voting Period:	See Appendix M
Target Population:	Neuchâtel Citizens ²⁴⁸
Channel:	Uncontrolled>Vote Data Return>Web Application
Technology Provider:	Scytl
Channel Protection:	The EAC was unable to obtain this information
Participating Voters:	See Appendix M
Authentication:	One-factor: Voter PIN

Neuchâtel contracted Scytl to assist in implementing their Internet voting system. The Scytl Pnyx.core platform is integrated into the Neuchâtel Internet voting portal titled “guichet sécurisé.”²⁴⁹ With the success of the initial pilots the Federal Chancellery accepted the Neuchâtel system for continuous use. Internet voting was implemented in an effort to reduce the costs associated with

Section 3: European Projects

conducting elections while maintaining the convenience of postal voting, which 90% of the canton votes by.²⁵⁰ The voter's PC requires a standard web-browser for the election. The voting system encrypts and digitally signs vote data on the voter's PC, before transmitting the data to a central server. Once received, voters are provided a cryptographic receipt that does not show their ballot selections.²⁵¹ A shuffling and decryption process is performed before the votes can be tabulated.

In order to cast a vote on the system a voter must:

- 1) Physically register to vote at a government office to receive a PIN code
- 2) Navigate to the Neuchâtel Internet voting portal
- 3) Input the PIN code
- 4) Make selections
- 5) Cast votes²⁵²

Standards Used

Although special standards were not required or used in implementing the system, the source code was audited by security experts hired by the Neuchâtel government.²⁵³ The Neuchâtel Government IT department certified the source code and digitally signed the binaries generated for the voting system's use. A continuous and random audit process is employed during and after elections to verify system integrity.²⁵⁴

Level of Risk Assumed

The EAC was unable to obtain this information.

Entity Assuming Risk

The Canton of Neuchâtel assumed the risk for the system.

Zurich

Sponsor:	The Statistical Office of the Canton Zurich
Election Type:	Referenda and Initiatives
Date or Voting Period:	See Appendix M
Target Population:	Zurich voters
Channel:	Uncontrolled>Vote Data Return>Web Application
Technology Provider:	Unisys
Channel Protection:	SSL
Participating Voters:	The EAC was unable to obtain this information
Authentication:	One-factor: Voter PIN

The Unisys Internet voting system used in Zurich was launched in 2002 at the same time as the systems used in Geneva and Neuchâtel.²⁵⁵ The system was first used in a student election, and subsequently used in a public election in Bulach in 2005. In the initial versions of the system voters could cast votes via personal computers and via SMS. In 2007, Zurich announced that it would discontinue using the SMS voting channel.²⁵⁶

Voting information is sent to voters six weeks before Election Day. The voting system uses a two-step encryption process. When a voter casts a ballot, the vote is encrypted on their computer. When it is received by the central server, it is decrypted, checked for structure and integrity, and then re-encrypted.²⁵⁷

To cast a ballot voters must:

- 1) Navigate to the appropriate web address
- 2) Input the voter identification number
- 3) Make ballot selections
- 4) Cast ballot
- 5) Enter the personal identification number
- 6) Compare the security symbol with the symbol the voter received in the mail²⁵⁸

Standards Used

E-voting through the Internet and with Mobile Phones, published by the Statistical Office in Zurich, states the following standards and documents were used in the construction and auditing of the voting system:

- The operational concept of the voting system is based on the IT infrastructure library (ITIL).

Section 3: European Projects

- The “security concept is defined according to ISO/IEC 17799 and BS7799 or higher.”²⁵⁹
- The ACM Statement on Voting Systems²⁶⁰

Level of Risk Assumed

“The certification of the hardware and its physical security environment had to be done in compliance with U.S. DoD level of protection of class B2 or lower.”²⁶¹

Entity Assuming Risk

The Canton of Zurich assumed the risk for the system.

United Kingdom

Sponsor:	Ministry of Justice; Electoral Commission
Election Type:	Local Elections
Date or Voting Period:	See tables 3-9, 3-11 and 3-14
Target Population:	General Electorate (England)
Channel:	Controlled and Uncontrolled forms of Internet voting. See tables 3-9, 3-11 and 3-14
Technology Provider:	See tables 3-9, 3-11 and 3-14
Channel Protection:	The EAC was unable to obtain this information
Participating Voters:	See tables 3-10, 3-12 and 3-13
Authentication:	One-factor and Two-factor (varies with provider)

The Electoral Commission, created in 2001 by a report from the Parliamentary Committee on Standards in Public Life, has two main objectives: to promote transparency and integrity in party and election finance; and to promote well run elections, referendums and electoral registration.²⁶² This mandate was set out in the *Political Parties, Elections and Referendums Act 2000*. The *Representation of the People’s Act 2000* outlines the process for pilot programs in Part 2, Section 10. This Act allows local jurisdictions to submit pilots to the Secretary of State for approval.

Between 2002 and 2007, the United Kingdom has conducted over thirty pilots utilizing different Internet voting channels including telephone and remote electronic voting from controlled and uncontrolled environments. The election jurisdictions administering the pilots often used dissimilar voting systems and often piloted multiple voting channels concurrently. The EAC was unsuccessful in

Section 3: European Projects

obtaining information on many of the individual pilots. However, the Electoral Commission conducted an analysis and published their findings on the 2002, 2003, and 2007 pilots. These reports are the EAC's source of information for the analysis of the Internet voting projects in the United Kingdom.

2002 Pilot Projects

In May 2002, nine polling locations enabled multi-channel and electronic voting pilot schemes.²⁶³ Table 3-9 is a list of locations and methods used during the 2002 pilots using Internet voting systems.

Table 3-9²⁶⁴ Location, Method and Provider

Date	Location	Voting Method	Technology Provider
April 26-May2, 2002	Liverpool City Council	Internet, Telephone and Text message	elections.com
April 26-May 2, 2002	Sheffield City Council	Internet, Text message and Kiosk	elections.com
April 25-27, 2002	St. Albans City & District	Internet, Telephone and Kiosk	Oracle
April 25-27, 2002	Crewe & Nantwich Borough Council	Internet and Kiosk	Oracle
April 26-30, 2002	Swindon Borough Council	Internet and Telephone	Votehere.net

Voters were able to cast ballots from their home computers and from computers available in controlled environments via touch screen machines or PCs in polling stations and other public areas.²⁶⁵ Postal voting and traditional methods were offered in addition to the pilot methods. All hardware and software performed successfully in the 2002 pilots.²⁶⁶ Each site and method used different types of verification, but all required a personal identification number and password.²⁶⁷

The process for voting in Liverpool was:

1. PINs, passwords, candidate codes, web address and instructions were sent out in a single mailing to 21,593 electors in Church and Everton wards.
2. To vote via the Internet:
 - a. The voter accessed the website and entered the PIN and password provided by the election office.

Section 3: European Projects

- b. Upon verification of the PIN and password, the voter viewed an on-screen ballot with screen prompts to assist with instructions.
 - c. The voter made their selections, confirmed the choices and submitted the vote.
 - d. The completed vote was transmitted to election.com's voting server via the Internet. The election.com system includes an Application Program Interface (API) enabling data from multiple channels to be integrated on the same secure voting platform.²⁶⁸
 - e. At the close of polls, data was loaded into an electronic tabulation system.
 3. To vote via telephone (available on mobile or touch tone):
 - a. The voter accessed the telephone voting system by entering the PIN and password provided by the election office.
 - b. An Interactive Voice Response (IVR) script gave candidate's names and descriptions matching the ballot layout.
 - c. Voters selected candidates by using buttons on the phone, per the instructions provided at the beginning of the call.
 - d. Voters were asked to confirm or cancel each selection; upon confirmation, the vote could not be changed.
 - e. The completed vote was held in election.com's voting server.
 - f. Results were loaded into a tabulation system upon the close of polls.
 4. To vote via SMS (Text):
 - a. Using the PIN, password and candidate codes, the voter created a text message:
`<PIN>`
`<PASSWORD>`
`<CANDIDATE NUMBER>`
 - b. The voter sends the message to the specific phone number assigned to their ward.
 - c. The voter received a text message response confirming the vote was received.
 - d. The completed vote was held in election.com's voting server.
 - e. Results were loaded into a tabulation system upon the close of polls.²⁶⁹

The process for voting in Sheffield was:

1. Poll cards were sent out to 34,456 electors in Hallam, Manor and Nether Edge wards. The poll card consisted of a smart card containing a PIN identifying the elector and their ward. The PIN was provided as a numeral and barcode.

Section 3: European Projects

2. The voter received a password, candidate codes and information on the e-voting options in the mailing containing the smartcard.
3. To vote via kiosk:
 - a. Voters swiped the poll card and entered the PIN to gain access to the system.
 - b. The voter navigated the screen and made their selections, confirming their vote upon completion of the ballot, prior to submitting the ballot.
 - c. The completed vote was transmitted to election.com's voting server via the Internet.
 - d. At the close of polls, data was loaded into an electronic tabulation system.
4. To vote via the Internet:
 - a. Followed the same process as Liverpool.
5. To vote via SMS (Text):
 - a. Followed the same process as Liverpool.²⁷⁰

The process for voting in St. Albans was:

1. Ten thousand electors in Sopwell and Verulam wards in St. Albans were mailed poll cards containing a 16 digit Voter Identification Number (VIN) prior to the voting period.
2. Following this initial mailing, officials sent PINs to each of the electors, to be used for Internet or telephone voting.
3. Electors were instructed to bring both items to the polling place with them.
4. To vote via kiosk:
 - a. Voters placed their VIN card under the screen, so the machine could read the number.
 - b. After scanning the VIN, the voter entered the PIN number provided by the election office.
 - c. Upon verification of the VIN and PIN, the candidate list was displayed to the voter.
 - d. Voters made their selections and confirmed their selections or could vote a blank ballot.
 - e. The completed vote was transmitted to BT's data store by an Integrated Services Digital Network (ISDN) connection to each kiosk.
 - f. Results were loaded into a tabulation system upon the close of polls.
5. To vote via the Internet:
 - a. Voters accessed the website; selected the instructions and language preferences; and entered their VIN and PIN numbers provided by the election office.

Section 3: European Projects

- b. Upon verification of the VIN and PIN, the candidate list was displayed.
 - c. Voters made their selections and confirmed their selections or could vote a blank ballot.
 - d. The completed vote was held in BT's secure data store.
 - e. Results were loaded into a tabulation system upon the close of polls.
6. To vote via telephone (available on mobile or touch tone):
- a. Voters called the access number provided; selected the instructions and language preferences; and entered their VIN and PIN numbers provided by the election office.
 - b. An IVR script gave candidate's names and descriptions matching the ballot layout.
 - c. Voters selected candidates by using buttons on the phone, per the instructions provided at the beginning of the call.
 - d. Voters were asked to confirm or cancel each selection; upon confirmation, the vote could not be changed.
 - e. The completed vote was held in BT's data store.
 - f. Results were loaded into a tabulation system upon the close of polls.²⁷¹

The process for voting in Crewe and Nantwich was:

1. Poll cards containing a 16 digit VIN were sent to the 7,641 voters in Maw Green and Wynbunbury wards prior to the voting period.
2. Following this initial mailing, officials sent PINs to each of the electors, to be used for Internet or telephone voting.
3. To vote via the Internet:
 - a. Followed the same process as St. Albans Council.²⁷²

The process for voting in Swindon was:

1. Packages including ballot codes, instructions and the voting website address were sent to 126,953 voters (19 out of 22 wards).
2. To vote via the Internet:
 - a. The voter accessed the website with the ballot code number.
 - b. Screen prompts assist voter navigation through the ballot. The voter cannot cast a blank ballot using the votehere.net system, meaning at least one vote must be recorded.
 - c. The completed and confirmed ballot was stored in a vote store.
 - d. Results were loaded into a tabulation system upon the close of polls.
3. To vote via telephone:

Section 3: European Projects

- a. Voters called in to a phone number given in the ballot code package delivered by the election office.
- b. An IVR script gave candidate's names and descriptions matching the ballot layout.
- c. Voters selected candidates by using buttons on the phone, per the instructions provided at the beginning of the call.
- d. Voters were asked to confirm or cancel each selection; upon confirmation, the vote could not be changed. Voters were unable to vote a blank ballot.
- e. The completed vote was held in a data store.
- f. Results were loaded into a tabulation system upon the close of polls. ²⁷³

The Electoral Commission provided the figures in Table 3-10, illustrating voter use during the 2002 pilots.

Table 3-10²⁷⁴ Channel Used by Voter in Each Location

Location	Polling Place/Postal	Internet	Telephone	Text
Liverpool City Council (2 wards)	3957 (59.4%)	1093 (16.4%)	1162 (17.4%)	445 (6.7%)
Sheffield City Council (3 wards)	8881 (67.7%)	2904 (22.1%)	--	1327 (10.1%)
St. Albans City & District (2 wards)	1539 (49.5%)	825 (26.5%)	744 (23.9%)	--
Crewe & Nantwich Borough Council (2 wards)	1839 (83.5%)	364 (16.5%)	--	--
Swindon Borough Council (19 wards)	33,329 (84.1%)	4293 (10.8%)	2028 (5.1%)	--
Total = 28 wards	49,545 (76.5%)	9479 (14.6%)	3934 (6.1%)	1772 (2.7%)

In the Electoral Commission's 2002 report, the Commission offered many recommendations. The following recommendations are most pertinent to this report's objectives:

Section 3: European Projects

- A need to create an integrated UK-wide pilot strategy in order to continue moving toward the implementation of an “e-enabled” voting system capable of handling a UK general election.
- Funding for future pilots should be provided by central government.
- Pilot application should not be approved unless they contribute to the development of the overarching goal of “e-enabled” voting.
- Testing should be conducted across whole authorities or constituencies to ensure they can operate in “real-life” circumstances.
- The Government should develop a high-level functional specification of what each type of voting or counting scheme should deliver.
- The Government should agree on formal security and control attributes against which each potential technical solution can be assessed.
- The Government should develop standard terms and conditions of contract to be used as the basis for negotiation with technology providers.
- Technology should provide opportunities to increase the security of elections and increase accessibility.
- Develop a set of technical criteria from 2002 evaluation to test and judge future pilots. ²⁷⁵

Standards Used

Amendments to the Representation of the People Act 2000 created the Electoral Commission and gave them a number of duties. One of those duties included evaluation of pilot scheme proposals for England, Wales and Scotland (at the request of the Scottish Government). The Electoral Commission was required to publish a report on each pilot scheme within 3 months after Election Day. After the 2002 pilots were conducted, the Electoral Commission highlighted a need for high-level functional specifications, testing criteria, and standardized terminology. This led to the creation of the *Statement of Requirements* document.

Level of Risk Assumed

The EAC was unable to obtain this information.

Entity Assuming Risk

The Ministry of Justice, Electoral Commission and local officials assumed the risk for the system.

2003 Pilot Projects

In 2003, 14 jurisdictions conducted pilots using some form of Internet voting. The participating jurisdictions selected their preferred supplier from a list provided by the Government. Table 3-11 outlines the locations and channels selected.

Section 3: European Projects

Table 3-11²⁷⁶ Location, Channel and Provider

Date (Close of Polls)	Location	Voting Method	Technology Provider
April 29, 2003	Stroud	Internet and Telephone	Athena
April 30, 2003	Swindon	Internet, Telephone and Digital TV	Athena
April 27, 2003	Kerrier	Internet, Telephone and Digital TV	Opt2Vote/Athena
April 27, 2003	Vale Royal	Internet and Telephone	Opt2Vote/Athena
May 1, 2003	Shrewsbury & Atcham	Internet, Telephone and Digital TV	Opt2Vote/DRS/Athena
April 29, 2003	Stratford on Avon	Internet and Kiosk	Strand/PowerVote/Athena
May 1, 2003	Ipswich	Internet, Telephone and Text message	Unisys
April 29, 2003	Norwich	Internet, Telephone and Text message	Unisys
May 1, 2003	Sheffield	Internet, Telephone, Text message and Kiosk	Unisys
May 1, 2003	South Somerset	Internet, Telephone and Kiosk	Unisys
May 1, 2003	St Albans	Internet, Telephone and Kiosk	Unisys
May 1, 2003	Chorley	Internet and Telephone	Unisys
May 1, 2003	Rushmoor	Internet	Unisys
May 1, 2003	South Tyneside	Internet, Telephone, Text message and Kiosk	Unisys

Of 17 pilots conducted in 2003, remote e-voting from uncontrolled PCs was provided in 14 pilots.²⁷⁷ Voters accessed the website and logged in to the system with credentials supplied in mailings from the local election office. Credentials were mailed to voters in mailings and consisted of a VIN and PIN, Voter ID and password, or PIN and password.²⁷⁸ Voters in Kerrier, Sheffield, Shrewsbury & Atcham, and Vale Royal received voter credentials in two mailings.²⁷⁹

Section 3: European Projects

If applicable, the voter chose their district or parish.²⁸⁰ The voter selected their choices, reviewed the ballot and casts the ballot. In five locations (Ipswich, Norwich, St Albans, South Somerset and Sheffield), the voter received a receipt ID to compare to the receipt ID on the poll card.²⁸¹ In one jurisdiction (Stratford on Avon), voters received a receipt they could compare to another page to confirm their ballot reached the ballot box.²⁸²

Most of the kiosk voting sites consisted of a PC residing in a “robust case” with an interface similar to that used by Internet voters.²⁸³ In St Albans, Sheffield, South Somerset and Swindon, the kiosks were online and connected to the same central servers as the other e-voting channels being used.²⁸⁴

The Electoral Commission provided the figures in Table 3-12 regarding voter use of multi-channel system for the 2003 pilots.

Table 3-12²⁸⁵ Voter Use of E-channels by Location

Location	Voter Use of E-channels
Stroud	20.3%
Swindon	24.5%
Kerrier	15.0%
Vale Royal	23.8%
Shrewsbury & Atcham	18.6%
Stratford on Avon	14.0%
Ipswich	21.7%
Norwich	10.0%
Sheffield	36.2%
South Somerset	16.2%
St Albans	36.2%
Chorley	12.7%
Rushmoor	15.0%
South Tyneside	11.0%

Table 3-13 details the percentage of voting carried out on the channels available during the pilot.

Table 3-13²⁸⁶ Voter Use of Channels Provided

Channel	Overall Usage	Usage of channel where available
Polling station (paper)	34.6%	67.6%
Postal voting	40.4%	40.4%
Internet	12.6%	12.6%
Telephone	6.5%	7.1%
Text message	1.4%	3.8%
Digital TV	0.2%	1.2%
Kiosk (only method available at polling place)	3.7%	77.3%
Kiosk (one of multiple channels available at polling place)	0.7%	1.3%
All remote e-channels	20.7%	N/A

Standards Used

The Government contracted with suppliers and the local authorities chose their provider. Unlike 2002, a *Statement of Requirement* consisting of 61 separate requirements was a central part of the procurement process.²⁸⁷ Based on experiences in 2003, the Electoral Commission made the following recommendations in its report, *The Shape of Elections to Come*:

- Technical Requirements for future e-enabled elections should be further developed and based on the existing “Statement of Requirements.” The requirements should clearly state the standard expected and controls should be implemented to promote adherence to the requirements. Specific requirements should include:
 - The need for protecting the server from malicious attack should be stated formally;
 - Requirements should state that each voter can only cast a single, valid vote;
 - Voter secrecy and ballot secrecy should be protected;
 - Information for production of poll cards should be protected;
 - Lost credentials should be managed securely and not just replaced;
 - Public verification of requirements must be clarified;

Section 3: European Projects

- Clearance levels for system operators should be defined;
- Remote administration of the central election platform should be prohibited;
- Generic threat and risk assessment of the e-voting process should provide guidance on security measure weaknesses.
- Votes should be digitally signed by the channel servers and information should be cross-checked to ensure integrity.
- Greater use of end-to-end encryption should be made across boundaries and support for this should be provided within the ISO Standard Election Markup Language (EML).
- The Returning Officer should hold the decryption key and have control of downloading the results.
- Voting credentials should be sent in two separate mailings and responsibility for assigning the credentials should be handled by the local authority.
- The use of multiple and redundant hosting and infrastructure should be considered in future pilots.
- A full risk assessment should be conducted for each e-voting service selected and used by a jurisdiction.
- Specific and proactive methods for measuring the number of attacks and the level of potential fraud should be required for future pilots.
- A single organization should take a leadership role for the end-to-end operation of each pilot scheme. Local authorities should have greater involvement in project management and oversight.
- More comprehensive training program provided for Returning Officers and their staff to help them fulfill their expanded role in oversight.²⁸⁸

Level of Risk Assumed

The EAC was unable to obtain this information.

Entity Assuming Risk

Ministry of Justice, Electoral Commission and local officials assumed the risk for the system.

2007 Pilot Projects

In 2007, seven applications were received, but only five pilots were accepted by the Electoral Commission due to unaddressed security concerns in the other two applications.²⁸⁹ Table 3-14 outlines the location and channels selected.

Section 3: European Projects

Table 3-14²⁹⁰ Location, Channel and Provider

Dates	Location	Voting Method	Technology Provider (Consortium)
April 26-May3, 2007	Rushmoor Borough Council	Remote Internet	ES&S
April 26-30, 2007	Sheffield City Council	Remote Internet & Telephone	Opt2Vote
April 26-May 1, 2007	Shrewsbury & Atcham Borough Council	Remote Internet & Telephone	Opt2Vote
April 26-May 3, 2007	South Bucks District Council	Remote Internet & Telephone	ES&S
April 26-May 3, 2007	Swindon Borough Council	Remote Internet & Telephone	Tata Consultancy Services

Standards Used

The *Statement of Requirements* was used in the procurement process.

Level of Risk Assumed

In the 2007 Electoral Commission Report the Electoral Commission stated that “there was an unnecessary high level of risk associated with all pilots and the testing, security and quality assurance adopted was insufficient.”²⁹¹ In the Report, the Commission recommended against further e-voting pilots until the following elements are in effect:

- Comprehensive electoral modernization framework covering the role of e-voting, including a clear vision, strategy and effective planning. The strategy should outline how the project will address transparency, public trust and cost.
- A central process must be implemented to ensure that local authorities have access to tested and approved e-voting solutions, either through an accreditation and certification process or through a more stringent procurement process.
- Sufficient time must be allocated for planning e-voting pilots.²⁹²

Entity Assuming Risk

Ministry of Justice, Electoral Commission and local officials assumed the risk for the systems.

Section 4 Canadian Projects

As of 2011, six Canadian provinces have passed legislation allowing for various forms of electronic voting, including Internet voting: Alberta, British Columbia, New Brunswick, Nova Scotia, Ontario and Saskatchewan.²⁹³ The EAC located information on three Canadian municipalities that implemented Internet voting: Markham, Peterborough, and Halifax. These systems were used in local elections in conjunction with other electronic voting technologies. Each municipality selected a different technology provider for their jurisdiction and administered the project independently. Table 4-1 provides a timeline of the three systems used in Canada:

Table 4-1²⁹⁴ *Timeline of System Use in Canada*

Year	Event
2003	First Markham Municipal Election
2006	Second Markham Municipal Election
2006	First Peterborough Municipal Election
2008	First Halifax Municipal Election
2009	Second Halifax Municipal Election
2010	Third Markham Municipal Election
2010	Second Peterborough Municipal Election

The Canadian federal government partnered with Elections-Canada to produce a study of the three municipalities' experiences, titled *A Comparative Assessment of Electronic Voting*. A list of risks associated with different types of electronic voting (e.g., remote electronic voting, kiosk voting over the Internet and telephone voting) is contrasted and compared in the study.²⁹⁵ The study contains additional information regarding other international Internet voting projects.

Halifax

Sponsor:	Halifax Regional Municipality
Election Type:	Municipal Elections
Date or Voting Period:	See Table 4-1
Target Population:	Halifax, Nova Scotia
Channel:	Uncontrolled>Vote Data Return>Web Application
Technology Provider:	Intelivote
Channel Protection:	SSL/TLS
Participating Voters:	2008: 28,709 via Internet and 2009: 3,259 via Internet ²⁹⁶
Authentication:	One-factor: PIN and Date of Birth ²⁹⁷

Halifax introduced Internet voting in 2008 as part of a pilot project. Internet voting and telephone voting channels were offered to voters. Halifax chose to use Intelivote’s Internet/phone voting system via an RFP process. Halifax did not require voters to specifically register to use the Internet voting system; instead, all voters were offered the option of using an assigned PIN (issued with voter cards) and their date of birth to authenticate to the system.²⁹⁸ In the 2008 Municipal and School Board Elections electronic voting was available only during a specified advanced voting period. In the 2009 Special Election (one district by-election) electronic voting was made available to voters during the entire voting period up to and including Election Day. Using this approach 74.2% of voters chose to cast their ballots electronically.²⁹⁹

Standards Used

The system instituted four “security checks”:

- penetration testing,
- analyzing the encryption system used to communicate between servers,
- an audit of the entire voting process, and
- analyzing the network’s overall security.³⁰⁰

Level of Risk Assumed

The Halifax Regional Municipality (HRM) also utilized the Town of Markham’s 2005 *Independent Risk Analysis on Alternative Voting Methods*.³⁰¹ HRM agreed that polling place voting is “clearly the least risky alternative”, and that postal voting is “clearly the most risky alternative.” To eliminate the need for voter registration for internet/phone voting and to mitigate the threat of notification cards being stolen in transit, HRM used the PIN and Date of Birth for authentication to the voting system. In addition, HRM sought changes to the

Section 4: Canadian Projects

Election Legislation that clearly outlined penalties for voter fraud in regard to Internet voting.

Entity Assuming Risk

Under the *Nova Scotia Municipal Elections Act* the Municipal Returning Officer is responsible for the assumption of risk associated with all aspects of the election including the use of electronic voting.³⁰²

Markham

Sponsor:	Town of Markham
Election Type:	Municipal Election
Date or Voting Period:	See Table 4-1
Target Population:	The EAC was unable to obtain this information
Channel:	Uncontrolled>Vote Data Return>Web Application
Technology Provider:	2003 & 2006: Election Systems and Software (ES&S), 2010: Intelivote ³⁰³
Channel Protection:	SSL/TLS
Participating Voters:	2003: 7,210; 2006: 10,639; 2010:
Authentication:	One-factor: Two PINs

Markham offered Internet voting for the first time in 2003, and continued the practice in 2006 and 2010. In addition to paper based polling place voting, Internet voting from the polling place and uncontrolled PCs was deployed during the early voting period.³⁰⁴ Voters using the Internet voting system were able to register to vote and cast a ballot from any PC.³⁰⁵ In 2003 and 2006, Election Systems and Software (ES&S) provided the Internet voting system and the electronic polling-place voting equipment. In 2010, ES&S provided electronic polling place voting equipment and Intelivote provided the Internet voting system.³⁰⁶

During the pre-election phase of the election process, all eligible voters received a voter information package. This package contained the registration PIN and the website address for the voting system.³⁰⁷ In order to cast a ballot a voter:

- 1) Registered to vote and created a personal passcode;
- 2) Received the Internet voting PIN;
- 3) Navigated to the appropriate URL;
- 4) Clicked a “vote” button;
- 5) Confirmed acknowledgement to a statement;

Section 4: Canadian Projects

- 6) Completed a CAPTCHA (an automated means of telling computers and humans apart);
- 7) Entered a personal passcode;
- 8) Entered the Internet voting PIN;
- 9) Made ballot selections;
- 10) Selected the “Vote Now” button.³⁰⁸

Standards Used

The Town of Markham published a *Request for Proposal* to solicit bids for an Internet voting system in 2010.³⁰⁹ The *Request for Proposal* listed a number of requirements, many relating to security and auditing functions, including:

- Online voting system must ensure a two-step process to register and vote (a. registration of intention to vote online and selection of a credential by the voter; and b. execution of vote following provision of credentials provided by the Town corroborated by voter’s registration credential). Proponents should include additional security options available;
- Online voting system must ensure that votes are verifiable. ToM [Town of Markham] should have a way to ensure that when user clicked for Candidate A, that the vote was recorded for Candidate A;
- Online voting system must not allow vote buying/selling;
- Online voting system must provide for secure identification and authentication of the information transmitted on the system;
- Online voting system must allow for digital signature by voter;
- Online voting system must ensure that voters will be protected against identity theft;
- Online voting system web-based interface must be via a web-browser in standard HTML and JavaScript. Solutions requiring the installation of an end-client or plug-in are not acceptable.³¹⁰

Security was not the only driving factor for the Town of Markham; accessibility played a key role in their selection of a voting system. The Town of Markham’s *Internet Voting Procedures* states:

The voter web user interface used by the Town’s INTERNET VOTING PROVIDER is coded with XHTML transitional document type and conforms to all W3C web standards. In addition, participants with visual disabilities can use select audio assistance on the registration screen and the voter entry screen to enter the required security CAPTCHA information.³¹¹

The *Internet Voting Procedures* document provided guidance on tabulation, recounts, security, and disruption of the voting process.

Level of Risk Assumed

In 2005, the Town of Markham commissioned an *Independent Risk Analysis on Alternative Voting Methods*. The study analyzed and compared the risks associated with polling-place voting, Internet voting, Internet voting with online voter registration, and postal voting.³¹² The study concluded that polling place voting is “clearly the least risky alternative”, and that postal voting is “clearly the most risky alternative.”³¹³ Internet voting, with voter registration as part of the voting system, was viewed as less risky than Internet voting without voter registration, because of the threat that the notification cards can be stolen while in transit in the postal system.³¹⁴

Entity Assuming Risk

The Town of Markham assumed the risk for the system.

Peterborough

Sponsor:	The City of Peterborough
Election Type:	Municipal Election
Date or Voting Period:	See Table 4-1
Target Population:	Peterborough, Ontario
Channel:	Uncontrolled>Vote Data Return>Web Application
Technology Provider:	Dominion Voting Systems
Channel Protection:	The EAC was unable to obtain this information
Participating Voters:	2006: 3,473; 2010: 3,951 ³¹⁵
Authentication:	One-factor: PIN and Date of Birth

Peterborough, Ontario introduced Internet voting in a 2006 Municipal Election after reviewing and learning of Markham's experiences with Internet voting.³¹⁶ Peterborough also conducted a 2010 Municipal Election via the Internet.³¹⁷ The municipality cited a reduced need for proxy voting applications, an opportunity to increase accessibility and lowering cost as reasons to implement the Internet voting system. Dominion Voting Systems provided the technology and the system allowed voters the opportunity to cast a ballot from any PC.

To use the system, voters registered with the City of Peterborough. Voters were offered the option of receiving their PIN via postal mail or email. All registered voters were mailed a registration card containing the appropriate login information for accessing and using the voting system.

Standards Used

These guiding principles were used when creating the system:

- Security
- Ease of use
- Service options/convenience
- Accessibility
- Enhanced features for voters with disabilities.³¹⁸

A security audit was performed by Digital Boundary Group in both 2006 and 2010.³¹⁹ The audit included an analysis of password strength and the security vulnerabilities present in the system. Peterborough decided to implement the system based on the results of the audit and Dominion's willingness to address suggested changes.³²⁰

Level of Risk Assumed

The EAC was unable to obtain this information.

Entity Assuming Risk

The City of Peterborough assumed the risk for the system.

Section 5 Oceanic Projects

Australia

Sponsor:	Joint Standing Committee on Electoral Matters, Australian Electoral Commission, Australian Defence Force
Election Type:	Federal Election
Date or Voting Period:	November 5-24, 2007
Target Population:	Australian Defence Force serving in selected locations
Channel:	Uncontrolled>Vote Data Return>Web Application
Technology Provider:	Registries Limited, Everyone Counts, Australian Government
Channel Protection:	Australian Defence Restricted Network and protocols
Participating Voters:	1,511 ³²¹
Authentication:	One-factor: PIN, Date of birth, name

In 2006, the Australian Government responded to a report provided by the Joint Standing Committee on Electoral Matters (JSCEM) which recommended consideration of remote electronic voting for certain voters, including Defence personnel serving overseas, by stating that a trial for remote electronic voting would be undertaken in the 2007 federal election.³²² The *Electoral and Referendum Legislation Amendment Act of 2007* enabled this trial to occur and was given royal assent in March 2007.³²³ This legislation allowed for a trial in 2007 only. Any subsequent trials would need to be supported by amended legislation. The trial was restricted to Australian Defence Force (ADF) personnel serving overseas in Afghanistan, Iraq, Timor-Leste and the Solomon Islands, who had access to the Defence Restricted Network (DRN).³²⁴

Registries Limited, working in conjunction with Everyone Counts, was selected to develop and pilot the remote electronic voting application.³²⁵ Throughout the design, pilot and testing process, the Australian Electoral Commission (AEC) and the ADF were an integral part of the process to ensure that the application met all policy and security requirements.³²⁶

The application was tested on multiple technology platforms and AEC and ADF conducted a comprehensive system acceptance process prior to production.³²⁷ During the 2007 election, 2,012 voters were registered to participate in this trial (80% of those eligible) and 1511 (75%) of those used the remote electronic voting system.³²⁸

Section 5: Oceanic Projects

Remote electronic voters were required to register to use the application. Defence provided Armed Forces Post Office (AFPO) addresses to AEC for validation of registration forms; if the applicant did not include one of these AFPO address, they were ineligible.³²⁹ After the application was approved, AEC staff produced a PIN and mailed the PIN and voting instructions to the remote voter.³³⁰

When the voter was ready to cast a ballot, they accessed the login screen on DRN and entered the required information.³³¹ A Java applet executed in the browser and offered the voter a list of lower House candidates whom the voter was required to rank in preference order.³³² Then the voter was offered the Upper House ballot in an adapted form of seeing it “above - line” or “below - line.”³³³ These sections of the ballot are usually shown together on paper, but the “above -line” allowed voters to choose a single group (i.e., party) and “below – line” allowed for individual candidate selection.³³⁴ After the voter completed their ballot, they were provided with a receipt to check and make sure their vote was received by the AEC database.³³⁵ A system architecture diagram is located in Appendix O.

The AEC project deployed polling place devices to 59 locations in Australia, which consisted of PCs running eVACs, a software program designed by SoftImp.com.au.³³⁶

Standards Used

The legislative basis and government approvals required for this pilot were:

- *Electoral and Referendum Legislation Amendment Act of 2007*
- *Joint Standing Committee on Electoral Matters’ recommendation 43 and AEC’s response (see AEC report)*
- *AEC & Defence’s joint recommendation to the Special Minister of State approved February 2007*
- *Royal Assent given March 2007*

To ensure security, the following design elements were required:

- a) The server storing the votes was housed in the AEC’s data center, although logically part of the DRN;
- b) Connectivity between the servers and Defence was via the Intra-government Communications Network in Canberra;
- c) Data on ICON was hardware encrypted;
- d) Access to the voting system was only available via the DRN.³³⁷

The AEC developed a *Statement of Requirements* which, among other things, required:

Section 5: Oceanic Projects

- a) Systems and associated security issues were specifically included in the SOR together with the methodology already determined to address these issues. Vendors were to confirm that they could meet the risk minimization or resolution in their responses.
- b) It was imperative that the acquired system operate within the DRN. To this end, the SOR required tenderers to provide a pilot system to determine compatibility of the offered software with Defence's various software levels.³³⁸

Level of Risk Assumed

Australian Standard 4360 was used. This standard was superseded by AS/NZS 31000:2009, or ISO 31000:2009. AS/NZS 31000:2009 provides generic guidelines and principles for risk management.

Entity Assuming Risk

The Australian Electoral Commission and the Australian Defence Force (Ministry of Defence), as well as the Australian government, accepted risk for this project. Managing the project and the relationship between AEC and ADF was quite complex and required a well defined project management plan.

This project was monitored and coordinated by the Project Board, which was jointly chaired by the First Assistant Commissioner Electoral Operations (AEC) and the Director General, Executive (ADF).³³⁹ The duties of the AEC/Defence Project Board included: overall direction of the project, ensure deliverables, arbitrate issues as they arise, and provide ministerial progress reports.³⁴⁰

State of New South Wales

Sponsor:	Premier of New South Wales, Electoral Commissioner
Election Type:	State Government Election
Date or Voting Period:	March 14-25, 2011
Target Population:	Low Vision, Disabled, and Absentee voters including those outside jurisdiction on Election Day
Channel:	Uncontrolled>Vote Data Return>Web Application/VOIP
Technology Provider:	Everyone Counts
Channel Protection:	SSL for online voting and all internal communication encrypted with standard industry approaches
Participating Voters:	46,864 total; 44,605 via Internet and 2,259 via IVR ³⁴¹
Authentication:	One-factor: PIN from voter and iVote number from system

Section 5: Oceanic Projects

In March 2010, the Premier of New South Wales (NSW) asked the Electoral Commissioner to investigate the possibility of providing Internet voting for blind or visually impaired voters in New South Wales.³⁴² The NSW Electoral Commission implemented the iVote system for the State Government Election in March 2011.³⁴³ The iVote system was designed for voters with disabilities; voters with blindness or low vision; illiterate voters; voters outside New South Wales on Election Day (absentee voters); and voters who live 20 km or more from a polling place.³⁴⁴

The iVote system allowed voting by two channels:

- Telephone voting via Public Switched Telephone Network (PSTN) with Dial-Tone Multi-Frequencing (DTMF) tones for voters to indicate voter intent; and
- Remote Electronic (Online) Voting in an uncontrolled environment over the internet.³⁴⁵

The iVote system allowed for online voter registration using a system developed by the New South Wales Electoral Commission. Everyone Counts provided the core of the voting system.³⁴⁶ Two geographically separate but identical data centers were used to host the application servers to run the iVote system. One application server was used to host the Internet-based web channel and another application server hosted the telephone channels.³⁴⁷ In addition to these application servers, database and logging/monitoring servers were also used.³⁴⁸ A system architecture diagram is located in Appendix P.

The elector registered to use the iVote system over the Internet or by calling an iVote call center operator.³⁴⁹ During the application process, the voter supplied a six digit PIN number.³⁵⁰ The Electoral Commission sent a letter to the elector to confirm registration.³⁵¹ The elector received an eight digit iVote number via email, mail, telephone or text.³⁵² When voting, the telephone system operated in a similar way to telephone banking services; Internet voting required the voter to logon and complete a ballot online using one of a range of web browsers.³⁵³ Upon completion of a voting session by phone or Internet, the elector received a receipt to allow them to later confirm their vote was counted.³⁵⁴

The iVote electronic ballot box was opened after the close of polls and all votes were decrypted and printed in one batch.³⁵⁵ Scrutineers were present to observe the unsealing and printing of iVote ballots; election officials with electronic keys opened the electronic ballot box.³⁵⁶

Table 5-1 shows voter turnout by voting channel and application:

Table 5-1³⁵⁷ Voter Turnout by Voting Channel

Criteria	Phone	Internet
Voters outside of New South Wales on Election Day (Absentee voters)	1,780	41,477
Voters 20km+ from Polling Place	101	1,542
Disabled voters	160	1,136
Blind, Low vision or illiterate voters	218	450
Total	2,259	44,605

Prior to implementation in the election, the New South Wales Electoral Commission released a *Technology Assisted Voting Audit: Pre-Implementation Report*. This audit focused on “a review and assessment of Electronic Voting Test Standard; Electronic Voting Test Strategy and Plan; Electronic Voting Test execution; Electronic Voting Business Continuity processes; and Electronic Voting Pre-Implementation readiness.”³⁵⁸ The testing standard was prepared by drawing on European and American standards for e-voting, which formed the basis of testing and conformance standards for the iVote system.³⁵⁹ Testing demonstrated that the system was accurate and met the standards, but there were several security vulnerabilities identified in security testing, which were either resolved or the risk was accepted prior to commencement of the election.³⁶⁰

Areas of critical focus were identified in the *Technology Assisted Voting Audit: Pre-Implementation Report* and the action taken was identified in the *Technology Assisted Voting Audit: Post-Implementation Report*. This document is available from the New South Wales Electoral Commission, along with the *Technology Assisted Voting Audit: Pre-Implementation Report*.

The *Technology Assisted Voting Audit: Post-Implementation Report* highlighted areas reviewed after implementation and found:

- No exceptions with the accuracy and completeness of votes cast via iVote occurred.
- A number of security risks were identified and accepted by the NSWEC, although none of these risks were exploited during the implementation.
- 1,062 voters were mistakenly given 7 digit iVote numbers instead of 8 digit iVote numbers; the iVote system did not prevent 182 voters from casting a vote using the 7 digit number. These votes were removed and electors were allowed to re-vote using a replacement 8 digit iVote

Section 5: Oceanic Projects

number. Although this was not discovered during testing, it did not affect the integrity of the election.

- A reminder intended for those who had registered but not yet voted, was mistakenly also sent to 842 electors who had already voted. Those who had voted were then sent confirmation that their ballot was actually received.
- The inter-site link between the two data centers failed, but voting was not impacted because all affected traffic was automatically routed through the Internet.
- The iVote web system experienced an 8 minute outage, but voting was only impacted for that period of time. The reason for the outage was not determined.
- Post election audit of an output file of votes showed the number of votes printed was not consistent with the number of votes contained in the decrypted voting file. It was found that a limited number of voters experienced a failure of Java Script on the iVote web page, which allowed a non-numeric character to be entered as ballot preference. Forty- three ballots were affected and the Electoral Commissioner made a determination on the affected votes.³⁶¹

Standards Used

The *Parliamentary Electorates and Elections Act 1912* was amended to require the “Electoral Commissioner to conduct an investigation as soon as possible into the feasibility of providing Internet voting for vision-impaired and other disabled persons for elections...and...to propose a detailed model of such Internet voting for adoption.”³⁶² Upon completion of the feasibility report, the recommendations of the report were introduced in the *Parliamentary Electorates and Elections Further Amendment Bill*, which passed in November 2010.³⁶³

The *Report on the Feasibility of Providing “iVote” Remote Electronic Voting System* provides a detailed system description and *Draft “iVote” Remote Electronic Voting System Requirements*.³⁶⁴ These requirements detail the function of different aspects of the voting system, including: the registration, Internet voting and telephone voting. Accessibility and Security requirements are also discussed (e.g., the system should meet or exceed World Wide Web Consortium Accessibility Group (WCAG AA) or similar standards).³⁶⁵

The NSWEC security requirements expect the system will at least demonstrate:

- Resistance to hacking of the server devices and/or a highly tamper-evident design
- In the case of home computer based voting, no information relating to a voting session shall remain on the computer once the session has been completed.

Section 5: Oceanic Projects

- Automatic measurement or assessment of the reliability of home computers.
- The system shall support scrutiny of the election process including possible deep audit by a NSWEC appointed auditor and/or specialist election scrutineers [sic] who may be members of the general public
- The iVote System shall be robust and secure to ensure a high level of availability during the voting period. There should be no single point of failure and no single storage location in the system design. The system should not be part of any shared infrastructure.
- No indeterminate states and no silent failures
- Elegant handling of voters who attempt to use unsupported browsers.
- The iVote system shall employ modern security techniques to ensure reliable and accurate operation and a security-in-depth design is preferred.
- Protections against insider attacks and/or tamper evident features
- Protections from attacks via the user's device (virus, etc.)
- Protections against various denial-of-service attacks or support for hardware and network protections that may be put in place in a web-hosting data center.³⁶⁶

NSW Electoral Commission instituted availability, security and privacy procedures:

- Development of an "iVote Standard" which combined best practices from a range of industry and electoral standards. This standard was used by the project team, to assess the system for operational suitability.
- External expert scrutiny and extensive testing, including intrusion testing and an involvement of independent auditors.
- Access by candidate scrutineers [sic], similar to other electoral processes.
- Sophisticated encryption to secure votes and automated processes to decrypt and print the votes in a way that ensures each elector's vote is secret.
- Parallel systems in different locations to ensure iVote should continue regardless of power failures, hacking attacks, equipment failures, etc.
- Procedures for the iVote and supporting manual processes were documented and formally approved by the Electoral Commissioner before publication on the Internet.³⁶⁷

Level of Risk Assumed

The *Report on the Feasibility of Providing "iVote" Remote Electronic Voting System* includes a table detailing risks and defenses for the project.³⁶⁸

Additionally, a Threat Analysis was performed, but it is not available to the general public.³⁶⁹

Section 5: Oceanic Projects

Additionally, NSWEC stated, with regard to risk:

To the extent possible, the iVote system should mirror the normal postal voting processes associated with a NSW General Election, which starts five days after the candidate nominations close and runs for almost two weeks to the Election Day (4th Saturday in March).³⁷⁰

The New South Wales Electoral Commission Risk Management Policy AS/NZS 31000:2009, or ISO 31000:2009, provides generic guidelines and principles for risk management.³⁷¹

Entity Assuming Risk

The NSWEC has “determined that the risks and issues associated with the security and scrutiny of a remote electronic voting system can be satisfactorily addressed.”³⁷²

Victoria

Sponsor:	Victoria Electoral Commission
Election Type:	2010 State Election
Date of Voting Period:	November 15-26, 2010
Target Population:	Voters with Disabilities, Voters from Culturally & Linguistically Diverse Backgrounds
Channel:	Controlled>Vote Data Return>VOIP/DRE/Kiosk
Technology Provider:	Hewlett Packard Australia and Scytl
Channel Protection:	The EAC was unable to locate this information
Participating Voters:	2010: 120 telephone, 841 kiosk
Authentication:	One-factor: <i>Telephone</i> : Code entered by polling place staff; <i>Kiosk</i> : smartcard for each voter session created by polling place staff

In 2006, Victoria ran a kiosk based pilot using Scytl technology to provide six voting centers with 36 non-networked PCs.³⁷³ The pilot was considered a success, with 199 votes cast via the kiosks.³⁷⁴ In the 2006 pilot, vote totals were returned to the VEC via sneakernet and this system is not considered part of the scope of this project.

In 2010, the Victorian Electoral Commission (VEC) rolled out Electronically Assisted Voting (EAV) devices to 100 early voting centers across Victoria, eight interstate voting sites and two centers in the United Kingdom.³⁷⁵ There are four

Section 5: Oceanic Projects

EAV components the Electoral Commission provided: EAV GSM telephone (cell phone), EAV SIP telephone (VOIP phone), EAV Issue point laptop (administrative device) and the EAV kiosk.³⁷⁶ Hewlett Packard Australia and Scytll were technology providers for the kiosk pilot in Victoria in 2006 and were retained to provide a phone voting interface system for the 2010 pilot.³⁷⁷ The system used in 2010 was the same software as the 2006 pilot, with updates and extensions.³⁷⁸ The VEC contracted for additional services including: voting kiosks design and construction; IVR phone hosting; penetration testing and Linux expertise; and software source code audit and trusted build control.³⁷⁹ The process of networking phones and kiosks in Victoria and the UK was a large undertaking and led the VEC to conclude that they should consider using a VPN over the Internet in the future, especially for voters outside of Victoria.³⁸⁰

Security cards and codes; kiosks; telephones; and network devices were distributed prior to the November 8th large scale test and remained in the field for the election.³⁸¹ When it was time to “go live” for the Election, staff swapped the test cards out with cards and codes held in a sealed envelope.³⁸² At the start of live voting, the central EAV server provided a “zero tally” to demonstrate it did not hold any votes.³⁸³ The VEC provided 302 telephones, which connected via a private network to an IVR service providing recorded instructions to guide voters through the ballot.³⁸⁴ The VEC provided 100 kiosks which provided visual and auditory guidance for the voter.³⁸⁵ Voters could access audio assistance in 12 languages on the phone and kiosk system.³⁸⁶

When the voter completed their ballot, the voter had an opportunity to review, verify and/or correct the ballot prior to casting their vote. Upon casting the ballot, the vote was encrypted by the IVR service or kiosk and sent to the VEC for printing and tabulation after the close of polls.³⁸⁷ The cryptographic keys were divided among a small group of VEC executives; these executives were also responsible for digitally signing the live election data after it was imported.³⁸⁸ The voter received a receipt to check the status of their ballot and could check their ballot on the VEC website after the close of polls.

The VEC did not target postal voters for the EAV pilot and if postal voters chose to use the EAV system, they were required to rescind their postal voter status.³⁸⁹ Only 120 eligible voters used the telephone voting method and 841 used the kiosks.³⁹⁰

Standards Used

The security goals for the system were: trusted operators were the only system operators; maintain hardware chain of custody and security of equipment; practical auditability and configuration of software; supervised support; proper password management; and votes remain secret, private and anonymous.³⁹¹

Prior to implementation, VEC conducted testing on the voting equipment focused on 200 requirements; although, only those requirements needing a

Section 5: Oceanic Projects

formal sign off were formally tested.³⁹² VEC testing focused on “User Acceptance Testing (UAT), usability, incremental integration, regression loops, network, technical acceptance...” and resulted in 300 formally documented tests.³⁹³ VEC contracted a “white hat hacker” to conduct penetration testing, who conducted end-to-end tests to expose vulnerabilities. The goal of penetration testing was to discover and remedy any weakness present in the system.³⁹⁴

A source code audit was conducted to “standards for secure coding concepts and good code layout.”³⁹⁵ Functional, accessibility and usability tests were conducted with the assistance of voters with disabilities. EAV had difficulty establishing and satisfying requirements for voters with multiple disabilities.³⁹⁶ Finally, automated testing, to gather large data sets, and “immersion testing,” or a dress rehearsal a week before Election Day, allowed the VEC to gather information and address any issues that came up prior to going live.³⁹⁷

Level of Risk Assumed

The VEC developed a Prince 2 Risk Register to document and track mitigation across all areas of the project and updated it to keep a running tally of active risks; a live reporting and alert system helped VEC keep a close watch on the system.³⁹⁸ The level of risk “was determined by assessing profiles for risk agents, attackers, operators, staff and the general public against possible risk management options and contingency planning.”³⁹⁹ Mitigations became the basis for the “Project burn list and software changes.”⁴⁰⁰ A project plan outlined deliverables and a Key Performance Indicator (KPI) list documented 90 project measures.⁴⁰¹ Many of the documents considered when evaluating risk came from the 2006 pilot project; however, some were taken from similar projects conducted in other locations, including: the *U.S. Department of Defense SERVE report*, *Parliamentary Inquiry 2005*, *Open Web Application Security Project Top Ten Risks*, AS/NZS 31000:2009, and the *Defence Signal Directorate Australian Government Information Security Manual*.⁴⁰²

Entity Assuming Risk

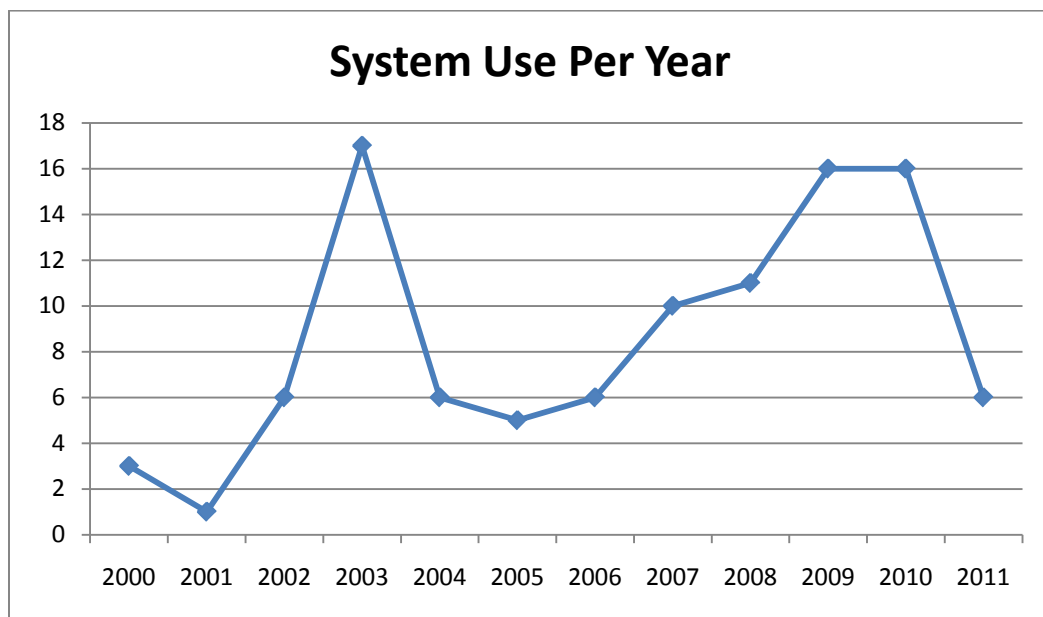
The Victorian Electoral Commission assumed the risk for this pilot project.

Section 6 Observations

This report presents a broad review of the Internet voting systems used in elections from January 2000 through November 2011. Projects in Canada, Europe, Oceania, and the United States were reviewed. This section discusses observations from the information gathered during the course of this research.

Within the data set, 31 projects in 13 countries were identified as using some form of Internet voting. The information used to construct these figures is included in Appendix Q. Figure 6-1 shows the Internet voting systems used, or scheduled for use, in elections by year.

Figure 6-1



To construct Figure 6-1, each instance of system use was counted for each election in which it was implemented. The Estonian system was counted four times, corresponding to its use in the 2005, 2007, 2009, and 2011 elections. West Virginia was counted twice, for two uses in 2010. DCBOEE, Norway, SERVE, and Sweden are not reflected in this diagram because their systems were not fielded. The sharp rise of system use from 2001 to 2003 voting reflects the increasing interest governments had in piloting Internet voting systems. The peak in 2010 can be attributed to a large number of first time projects (i.e., Oregon, West Virginia, DC, and Victoria), many of them based within the United States.

Figure 6-1 shows an increasing trend in the implementation of Internet voting systems since the year 2000. In 2003, the UK implemented 14 pilot projects, resulting in highest use of Internet voting systems worldwide. At publication,

Section 6: Observations

Norway is scheduled to pilot a system in late August 2011. It is possible that more system uses will occur in 2011, impacting the data of Figure 6-1.

Figure 6-2 shows the 31 projects divided into the four geographic regions this report surveyed.

Figure 6-2

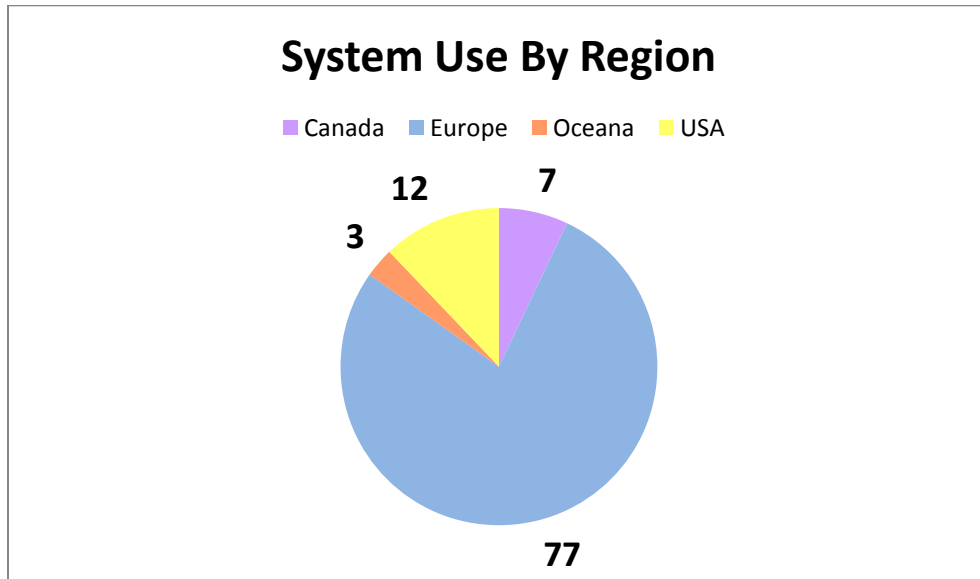
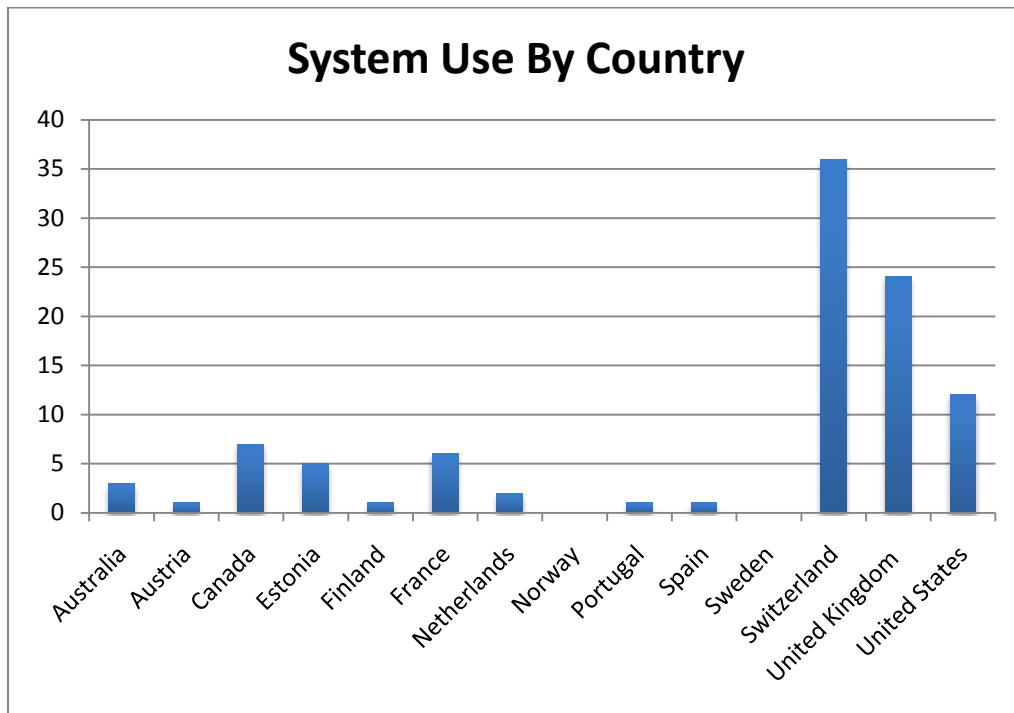


Figure 6-2 shows that Europe performed more Internet voting projects than any of the other regions surveyed.

Figure 6-3



Section 6: Observations

Figure 6-3 shows the data of the number of systems used by each country. Switzerland, overall implemented more Internet voting projects than any other nation with 36 system uses. The United Kingdom performed the second largest number of system uses with a total of 24.

Figure 6-4 shows the total number of system uses by project.

Figure 6-4

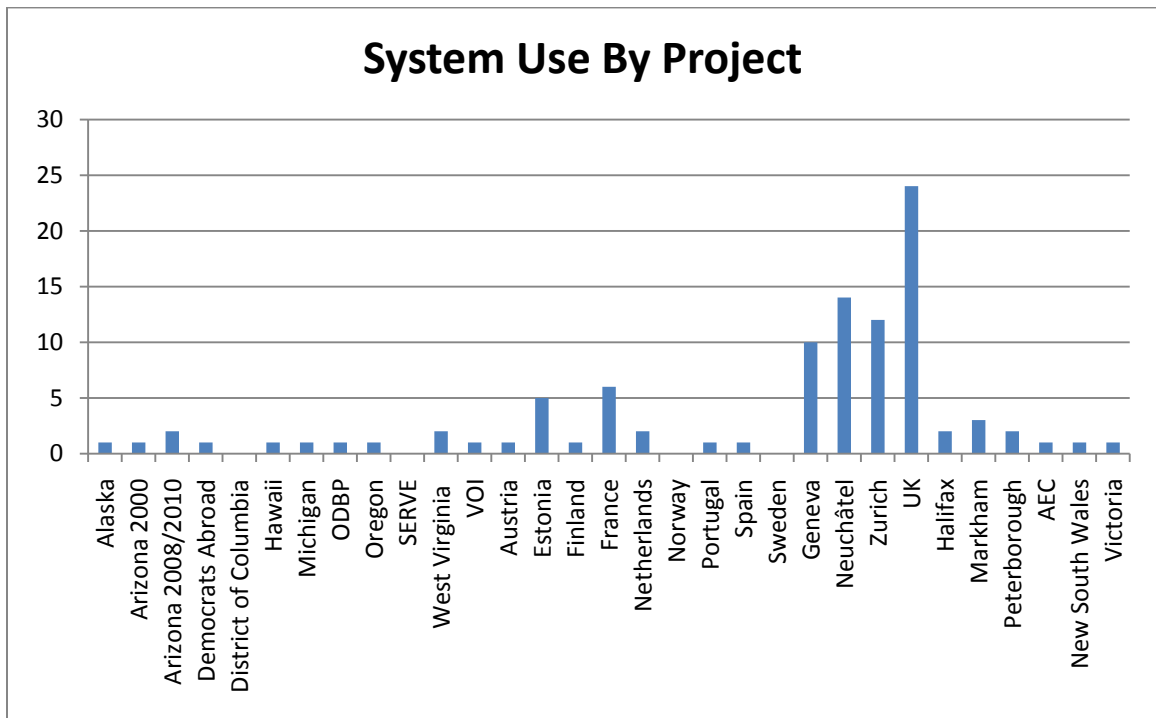


Figure 6-4 was constructed in the same manner as 6-1, by plotting each time a system was utilized in a project. Over half of the 31 projects were used only a single time. The data indicates that most systems were either not intended for continuous use or some other factor (i.e. information or experiences gained while piloting a system) led to the decision to discontinue implementation of the system.

As noted within project sections 2 - 5, the following factors are reasons for discontinuing Internet voting projects: legislation, technical factors, and public opinion. The AEC was unable to continue with their project because the original legislation was limited to a single year, and any future projects would need to have new authorizing legislation. Finland experienced technical difficulties, which led to the system inaccurately reporting vote totals. In the Netherlands, a group of citizens influenced public opinion by protesting, leading to the discontinuation of the RIES system. A similar situation was experienced in SERVE, with a number of computer scientists writing a report that was one of the factors leading to the discontinuation of the project. Though federal legislation allowing

Section 6: Observations

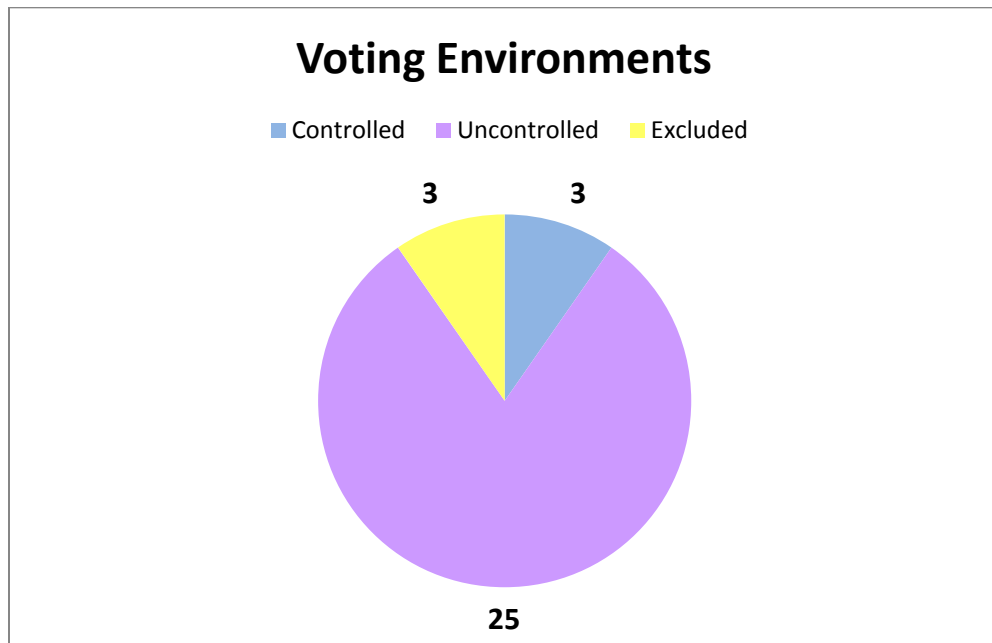
Internet voting pilots was introduced in the United Kingdom, the government ultimately decided to discontinue these pilots because, “there was an unnecessary high level of risk associated with all pilots and the testing, security, and quality assurance adopted was insufficient.”⁴⁰³

Switzerland and Estonia introduced Internet voting through federal legislation. In contrast to the United Kingdom, however, both Switzerland and Estonia have developed these pilots into continuous use systems. Notably, Switzerland has conducted more elections using Internet voting systems than any other location in the world.

Implementation

Twenty-six projects were conducted by a government entity. Five were sponsored by political parties for primary elections. The focus of this discussion is on the government projects. Only three of the projects, namely Finland, ODBP, and Victoria, employed system architecture with a controlled voting environment. Figure 6-4 compares the number of projects using controlled environments against the number using uncontrolled environments.

Figure 6-4



Sweden, the UK, and France were excluded from Figure 6-4 because there was either no system to analyze or the projects were composed of many dissimilar systems. Finland placed electronic voting machines in polling places connected to the Internet. ODBP set up supervised voting locations and provided the voting computers. Victoria used Voice Over Internet Protocol (VOIP) telephone voting devices in early voting centers set up in Australia and the UK. Controlled environment systems are considered to be lower risk than uncontrolled

Section 6: Observations

environment architectures.⁴⁰⁴ But to date, it appears that systems with controlled architectures may be used significantly less than systems utilizing uncontrolled architectures. The EAC has developed a standard to test and certify controlled environment systems, titled the *Pilot Program Testing Requirements*.⁴⁰⁵

The systems that have been used on a regular basis in binding elections all employ architectures with uncontrolled voting environments. These are Arizona (2008/2010), Estonia (2005, 2007, 2009, 2011), France (2003, 2006, 2009), Geneva (2010, 2011), Neuchâtel (2010, 2011), and Zurich (2010, 2011). The Arizona system enables a remote voter to upload their voted ballot to a secure server and was intended to be an ongoing alternative channel when it was developed. The Estonian system was also intended for continuing use when it was developed. The Swiss systems were developed under a federal government initiative to examine the feasibility of Internet voting as a new voting channel. The French system has been used in three consecutive elections by overseas absentee voters. All of these systems allow for voting from a remote computer. NIST has evaluated this architecture as having the highest threat profile in *NIST Threat Analysis of UOCAVA Voting Systems*.⁴⁰⁶

In all the projects other voting channels were available; Internet voting was provided as an alternative to existing voting methods. From the information available, it does not appear that any entity has considered Internet voting as a replacement for an existing voting channel. Projects were undertaken for one or more of the following reasons:

- 1) to evaluate potential as a new voting channel for general electorate
(Norway, Sweden, Switzerland, UK)
- 2) to evaluate as alternative to mail for overseas absentee voters
(Arizona, Australia AEC, D.C., France, Netherlands, New South Wales, ODBP, Portugal, SERVE, Spain, VOI, West Virginia)
- 3) to evaluate as alternative to paper ballots for voters with disabilities
(Markham, New South Wales, Peterborough, Victoria)
- 4) lower cost than mail voting, ease of use for voters
(All primaries, Honolulu, Neuchâtel, Peterborough, Spain)
- 5) increase voter turnout
(Alaska, Democrats Abroad, France overseas voter projects)

Most of the projects were implemented for only one or two elections. There are several reasons for this:

- 1) Project was 'proof of concept' and not intended for long term use
(SERVE, VOI)

Section 6: Observations

- 2) Project was one element of larger government initiative to explore technology
(Norway, Sweden, Switzerland, UK)
- 3) Authorizing legislation only for limited period
(Australia AEC, Victoria)
- 4) Problems experienced in pilot
(DCBOEE, Finland)
- 5) Public opposition to Internet voting
(Finland, SERVE)

There is nothing new about election officials evaluating new voting technologies as they become available. However, the decision to adopt Internet voting technology is different in kind from previous voting system choices because the technology is radically different from what has come before. With Direct Record Electronic and Optical Scan technology, an election official was considering discrete voting machines operated in isolation in protected physical spaces. As illustrated by many of the projects reviewed, Internet voting involves a complex distributed information technology system employing networks, servers, secure data centers, cryptography, and electronic identification and authentication methods. Adopting this method of voting means a paradigm shift in the way systems are procured, managed and administered.

Technically complex systems often use international standards to inform their development and procurement. Testing and formal certification programs can validate that complex systems conform to these standards. Due to their complexity, Internet systems are subject to different types of threats than current voting technologies such as DREs and optical scan systems. These threats will evolve over the life of the system. Consequently, a formal risk assessment and management process is an important aspect of system administration. These topics are further discussed in the following sections.

Standards and Requirements

In the United States, comprehensive standards are used for testing and certifying electronic voting systems, such as the *1990 Voting Systems Standards (1990 VSS)*, the *Florida Voting Systems Standards (FVSS)*, and the *2002 Voting System Standards (2002 VSS)*. The *2005 Voluntary Voting System Guidelines (2005 VVSG)*, which is the current standard used to test voting systems at a federal level includes requirements for accessibility, security, and other voting-specific functionalities. This standard does not include requirements to test and certify Internet voting systems, although the standard does not explicitly prohibit the use of Internet voting systems either. Locating standards and requirements

Section 6: Observations

utilized by other locations in the development of their systems assisted the EAC in its mandate of creating electronic absentee voting guidelines.

Currently, a single comprehensive standard for developing and testing Internet voting systems does not exist. Pilot project sponsors often drew heavily from variety of standards and requirements to develop and implement Internet voting systems. The majority of systems were not developed or tested to a single standard; often several standards, supplemented with additional requirements, were used. Many of the standards used in the projects addressed a specific area (e.g., accessibility or security) which are not specifically intended for voting systems. The *Council of Europe’s Legal, Operational, and Technical Standard for E-voting*, *FVSS*, and *1990 VSS* address voting-specific functions (e.g., ballot presentation and tabulation logic) in addition to accessibility and security. Voting-specific functionality differs from location to location, because the voting functions required to run an election vary. The Council of Europe, the Florida Secretary of State’s Office, the Australian Election Commission, and the United Kingdom’s Electoral Commission all created standards, which include voting specific functionality, accessibility and security requirements.

The requirements and expectations for accessibility vary widely, as locations have different definitions and legal mandates for the level of accessibility required in voting systems. Alternatively, the need to maintain security in information systems, such as electronic voting systems, exists worldwide. Table 6-1 provides the security standards used in each Internet voting system.

Table 6-1 Security Standards

Standard	Title
AS/NZS 31000:2009 (ISO 3100:2009)	<i>Risk management—Principles and guidelines</i>
ISO 27001	<i>Information Technology - Security Techniques - Information Security Management Systems - Requirements</i>
ISO 27002	<i>Code of practice for information security management</i>
ISO/IEC 15408	<i>Evaluation Criteria for Information Technology Security</i>
ISO/IEC 17799	<i>Information Technology - Code of practice for information security management (Renamed to ISO 27002)</i>
BS7799	<i>Guidelines for Information Security Risk Management (Renamed to ISO 27001)</i>

Locations that did not develop or use formal standards often created ad hoc requirements systems must meet. These requirements may be legally mandated or part of a Request for Proposal (RFP) process. The Swiss federal government mandated a list of requirements for the participating cantons; while Markham

Section 6: Observations

and Honolulu used RFPs to guarantee certain functionality within their systems. Estonia created a Working Group that developed a set of requirements for the country's Internet voting system.

Certification, expert review, and public scrutiny can be an alternative or additional method of verifying certain levels of functionality, accessibility, or security are present before the system is used. Some form of certification occurred in AEC, Austria, ODBP, SERVE, and VOI. Expert review occurred in a number of projects-Austria, Finland, ODBP, SERVE and Victoria-which allowed an outside organization, such as a university, laboratory, or a contractor to review portions of the system before it is used. In DCBOEE, Netherlands, and Norway the system's source code was available for public scrutiny.

Addressing Risk

Risk is a difficult concept to express, understand and measure. This is apparent in the means used to address risk from one project to the next. The EAC has knowledge of 13 formal risk assessments, and seven of these risk assessments are publicly available. Nearly every project used a different assessment methodology to measure risk.

In some instances, projects compared the risks associated with various forms of Internet voting with the risks of other, more traditional voting channels. At least seven projects - Austria, DCBOEE, Geneva, Honolulu, NSW, SERVE and VOI - decided to compare the risks associated with their Internet voting projects to the risks associated with postal voting. For example, Geneva listed the risks associated with their traditional voting channel alongside the risks associated with their proposed Internet voting system. If a risk existed in both channels, it was deemed acceptable. The DCBOEE employed a similar methodology, with the additional goal of limiting the introduction of new threats to the voting process. If new threats were introduced, they were mitigated in some way. To apply this methodology to systems used by United States military and overseas voters, a detailed risk assessment on the postal voting system in the United States is needed. As a first step, the EAC released a whitepaper titled *Uniformed and Overseas Citizens Absentee Voting Act Registration and Voting Processes* detailing the current postal voting system in the United States.⁴⁰⁷

The EAC is in the final stages of approving a risk assessment methodology for assessing the risks associated with multiple voting channels, known as the *Election Operations Assessment (EOA)*. It includes a user tutorial and a set of risk scenarios and assessment templates, which can be used without expert assistance. The risk scenarios can be modified and additional scenarios added, as necessary, for any type of voting channel or risk environment. One of the features of this tool is that it captures the assumptions made by the users when assigning risk values. This allows for the assumptions and risk values to be changed and the risk assessment run again to provide a sensitivity analysis of the

results. Once published, the EOA will provide a useful tool for jurisdictions and other interested parties to perform voting system risk assessments.

Final Thoughts

After collecting and reviewing information for the projects highlighted in this report, the following areas remain open for discussion and analysis:

- Closer analysis of voting protocols used by Internet voting systems may be necessary to understand the security benefits provided by each voting protocol.
- There may be a need for an international standard solely dedicated to Internet voting in an uncontrolled environment.
- There may be a need for a standard risk assessment methodology that local, state, and federal jurisdictions can follow.
- A uniform risk assessment methodology for all voting channels may be necessary for a comparison of the risks associated with each voting channel. Each project managed risks and the technical challenges of Internet voting in their own way.
- A dedicated forum or organization for communicating experiences or sharing information about Internet voting projects and/or innovations may need to be developed. A forum could facilitate discussion regarding obstacles and innovations in Internet voting; the creation of a standardized language to discuss Internet voting; best practices learned from those implementing pilots and continuous use systems; and an accurate history of the development of Internet voting.

Appendix A: Bibliography

The Bibliography contains all books, journal, reports and websites cited in the document. A source file of all cited documents is available at www.eac.gov.

Aaltonen, Jussi. "eVoting 2008: Statistics." Presentation at Ministry of Justice, Helsinki, Finland.

Alvarez, R. Michael and Thad E. Hall. *Point, Click and Vote: The Future of Internet Voting*. Washington, D.C.: Brookings Institution Press, 2004.

Arizona Secretary of State's Office. *Arizona's Military and Overseas System*, by Craig Stender. April 19, 2009.

Australian Electoral Commission. *eVolution not Revolution: Electronic Voting Status Report*. Parkes ACT, Australia: September 2002.

Australian Electoral Commission. *Report into Remote Electronic Voting at the 2007 Federal Election for Overseas Australian Defence Force Personnel*. Parkes ACT, Australia: April 18, 2010.

Beroggi, Giampiero. "Secure and Easy Internet Voting." *Computer (IEEE Magazine)*: February 2008.

Beroggi Giampiero. "E-Voting through the Internet and with Mobile Phones." *United Nations Public Administration Network*.
<http://unpan1.un.org/intradoc/groups/public/documents/unpan/unpan030950.pdf>
(accessed May 25, 2011).

Bundesministerium für Wissenschaft und Forschung. *E-Voting bei den Hochschülerinnen- und Hochschülerschaftswahlen 2009*. March 29, 2010.

California Internet Voting Task Force. *A Report On the Feasibility of Internet Voting* by Bill Jones. Sacramento, California, January, 2000.

Canada-Europe Transatlantic Dialogue. *A Comparative Assessment of Electronic Voting*. Ottawa, Ontario: February 2010.

Cervelló, Gerard. "The E-Participation Project of Neuchâtel." *European Journal of ePractice*: March 2009.

Chevallier, Michel. *Internet Voting: Situation Perspectives and Issues*. Geneva State Chancellery, received July 24, 2010.

Chevallier, Michel. *e-Voting Certification Project, Voting via the Internet*. Geneva State Chancellery, November 11, 2008.

City and County of Honolulu. *Notice of Request for Proposals (RFP-MAY-0900016)*. Honolulu, Hawaii: February 23, 2009.

Appendix A: Bibliography

City and County of Honolulu. *Proposal Document No. RFP-MAY-0900016 for On-Line Voting Services for the 2009 Neighborhood Board Elections for the Neighborhood Commission City and County of Honolulu*. Honolulu, Hawaii: March 20, 2009.

Clarkson, Michael, Brian Hay, Meador Inge, Abhi Shelat, David Wagner, and Alec Yasinsac. *Software Review and Security Analysis of Scytl Remote Voting Software*. Tallahassee, Florida: Florida State University's (FSU) Security and Assurance in Information Technology (SAIT) Laboratory, September 19, 2008.

Corporation of the Town of Markham. Request for Proposal 339-R-09: Vote Tabulation Systems and Integrated Voting Platform.

Cunha, João Falcão e, Mário Jorge Leitão, João Pascoal Faria, Miguel Pimenta Montiero, and Maria Antónia Carravilla. "A Methodology for Auditing e-Voting Processes and Systems used at the Elections for the Portuguese Parliament." *Electronic Voting 2006: Lecture Notes in Informatics* by Robert Krimmer (ed.), August 2-4, 2006.

Department of Defense. *Voting Over the Internet Pilot Project Assessment Report*. Prepared by the Federal Voting Assistance Program (FVAP). Washington, D.C.: June 2001.

Democrats Abroad. *Global Presidential Primary – Results Report*. Washington, D.C: February 21, 2008.

Electoral Commission (UK). "The Electoral Commission Website." Electoral Commission United Kingdom. <http://www.electoralcommission.org.uk/> (accessed May 2011).

Electoral Commission (UK). *Modernising Elections: A Strategic Evaluation of the 2002 Electoral Pilot Schemes*. London, England: August 2002.

Electoral Commission (UK). *The Shape of Elections to Come: A Strategic Evaluation of the 2003 Electoral Pilot Schemes*. London, England: July 2003.

Electoral Commission (UK). *Electronic Voting: May 2007 Electoral Pilot Schemes*. London, England: May 2007.

Ehringfeld, Andreas, Larissa Naber, Thomas Grechenig, Robert Krimmer, Markus Traxl, Gerald Fischer. "Analysis of Recommendation Rec(2004)11 Based on the Experiences of Specific Attacks Against the First Legally Binding Implementation of E-Voting in Austria." Presentation at the EVOTE2010 conference, Lochau/Bregenz, Austria, July 22, 2010.

Florida Department of State. *Florida Administrative Code: Rule 1S-2.030*. Tallahassee, Florida: September 13, 2004.

Florida Department of State. *Provisional Qualification Test Report: Scytl Release 1.0, Version 1*. Tallahassee, Florida: September 23, 2008.

Gerlach, Jan and Urs Gasser. "Three Case Studies from Switzerland: E-Voting." *Internet and Democracy Case Study Series*: March 2009.

Gjøsteen, Kristian. "Analysis of an Internet Voting Protocol." *Cryptology ePrint Archive* (July 7, 2010): <http://eprint.iacr.org/2010/380.pdf> (accessed June 9, 2011).

Appendix A: Bibliography

Jefferson, David, Aviel Rubin, Barbara Simons, and David Wagner. *A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)*. January 21, 2004.

Kahn, Robert E. and Vinton G Cerf. "What is the Internet (and What Makes it Work)." Internet Policy Institute, Washington, D.C., December 2009.

Katholieke Universiteit Leuven. *BeVoting Study of Electronic Voting Systems*. Leuven, Belgium: April 15, 2007.

Kim, Henry. Risk Analysis of Traditional, Internet, and Other Types of Voting Alternatives for Town of Markham. Markham, Ontario: June 23, 2005.

Krimmer, Robert. "Implementing Electronic Voting: The Austrian Experience." Lecture given at TED summer school, Varenna, Italy, September 7-13, 2003.

Krimmer, Robert, Andreas Ehringfeld, and Markus Traxl. "The Use of E-Voting in the Federation of Students' Elections 2009." Presentation at the EVOTE2010 conference, Lochau/Bregenz, Austria, July 22, 2010.

Krimmer, Robert and Gregor Wenda. "Electronic Voting in Austria: Experiences and Challenges." Presentation in Oslo, Norway, March 19, 2010.

McKinstry, John. "Peterborough's Experience with Internet Voting." Lecture, Policy Workshop – Internet Voting: What can Canada Learn?, Carleton University, January 26, 2010.

Mellet, Cathy. "HRM's Experience with Electronic Voting." Lecture, Policy Workshop – Internet Voting: What can Canada Learn?, Carleton University, January 2010.

Ministry of Justice (Finland). *Electronic Voting Pilot in the 2008 Municipal Elections* by Jussi Aaltonen. Helsinki, Finland: November 4, 2010.

Ministry of Justice (Finland). "Only Supervised Voting Allowed - Electronic Voting 2008." Ministry of Justice. <http://www.vaalit.fi/sahkoinenaanestaminen/en/valvotusti.html> (access June 15, 2011).

Ministry of Justice (Finland). "The Voting Process - Electronic Voting 2008." Ministry of Justice. http://www.vaalit.fi/sahkoinenaanestaminen/en/aanestyksen_kulku.html (access June 15, 2011).

Ministry of Justice (Finland).

"Why has Internet voting not been arranged? – Electronic Voting 2008." Ministry of Justice. <http://www.vaalit.fi/sahkoinenaanestaminen/en/ukk/ukk20.html> (accessed June 15, 2011).

Ministry of Justice, Election Technique Commission (Sweden). Excerpts from Technology and Administration in Election Procedure Final Report from the Election Technique 2000 Commission. Stockholm, Sweden: 2000.

Ministry of Local Government and Regional Development (Norway). "11 Municipalities to Try Out E-Voting in 2011." Ministry of Local Government and Regional Development (Norway).

Appendix A: Bibliography

<http://www.regjeringen.no/en/dep/krd/pressesenter/pressemeldinger/2010/11-kommunar-far-prove-e-val-i-2011.html?id=591610> (accessed June 9, 2011).

Ministry of Local Government and Regional Development (Norway). *Electronic voting—challenges and opportunities*. Oslo, Norway: 2006.

Ministry of Local Government and Regional Development (Norway.) “Evote 2011 Project.” Ministry of Local Government and Regional Development (Norway). <http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project.html?id=597658> (accessed June 9, 2011).

Ministry of Local Government and Regional Development (Norway). *E-vote 2011: Election system with Solution for Electronic Voting, Norway 2011*. Oslo, Norway: 2009.

Ministry of Local Government and Regional Development (Norway). *e-Vote 2011 Security Objectives*. Oslo, Norway: September 25, 2009.

Ministry of Local Government and Regional Development (Norway). *E-vote 2011 System Architecture Overview, Interfaces and Deployment V 1.3*. Oslo, Norway: June 13, 2011.

Ministry of Local Government and Regional Development (Norway). *E-vote 2011 System Architecture Overview, Interfaces and Deployment V 1.5*. Oslo, Norway: April 25, 2011.

Ministry of Local Government and Regional Development (Norway). *E-vote 2011: System Requirements Specification*. Oslo, Norway: September 10, 2009.

Ministry of Science, Technology and Higher Education (Portugal). “Electronic Voting Experiments in Political Elections Around the World.” Knowledge Science Agency website, http://www.english.umic.pt/index.php?option=com_content&task=view&id=3113&itemid (accessed March 16, 2011).

National Electoral Committee (Estonia). *E-Voting Conception Security: Analysis and Measures* by Arne Ansper, Anto Buldas, Mart Oruaas, Jaan Priisalu, Anto Veldre, Jan Willemson, and Kaur Virunurm. Tallinn, Estonia: December 15, 2003.

National Electoral Committee (Estonia). *Internet Voting in Estonia*. Tallinn, Estonia: 2007.

National Science Foundation. *Report of the National Workshop On Internet Voting: Issues and Research Agenda*. Arlington, Virginia, March, 2001.

National Institute of Standards and Technology (NIST). *Security Considerations for Remote Electronic UOCAVA Voting* by Nelson Hastings, Rene Peralta, Stefan Popoveniuc and Andrew Regenscheid. Gaithersburg, Maryland, February, 2011.

National Institute of Standards and Technology (NIST). *Threat Analysis on UOCAVA Voting Systems* by Andrew Regenscheid and Nelson Hastings. Gaithersburg, Maryland, December 2008.

Appendix A: Bibliography

- New South Wales Electoral Commission. "iVote Background." NSWEC. <http://www.elections.nsw.gov.au/voting/ivote/background> (accessed May 19, 2011).
- New South Wales Electoral Commission. "iVote Overview." NSWEC. <http://www.elections.nsw.gov.au/voting/ivote/overview> (accessed May 19, 2011).
- New South Wales Electoral Commission. *Report on the Feasibility of Providing "iVote" Remote Electronic Voting System*. Sydney, Australia: July 23, 2010.
- New South Wales Electoral Commission. *Technology Assisted Voting Audit: Post-Implementation Report*. Sydney, Australia: June 2011.
- New South Wales Electoral Commission. *Technology Assisted Voting Audit: Pre-Implementation Report*. Sydney, Australia: March 7, 2011.
- Nore, Henrik. "Open Source Remote Electronic Voting in Norway." Presentation at the OSCE Chairmanship Seminar, Working Session III, Vienna, Austria, September 17, 2010.
- Office for Democratic Institutions and Human Rights. *OSCE/ODIHR Election Assessment Mission Report: The Netherlands Parliamentary Elections 22 November 2006*. Vienna, Austria: March 12, 2007.
- Office of the Returning Officer (Markham). *Internet Voting Procedures*. Markham, Ontario: July 22, 2010.
- Ohlin, Tomas and Markus Hällgren. "Internet Voting in Practice: The Case of the Umeå Student Union." *e-Service Journal*: Fall 2002.
- Operation BRAVO Foundation. *Procedures and System Description for Secure Remote Electronic Transmission of Ballots for Overseas Civilian and Military Voters*. Arlington, Virginia: Operation BRAVO Foundation, June 19, 2008.
- Pont, Piet. "RIES Facts and Features Sheet." http://csrc.nist.gov/groups/ST/UOCAVA/2010/PositionPapers/PIET_PONT_RIES_UOCAVA.pdf (accessed June 6, 2011).
- Pont, Piet. "Election through the Internet: Can it be Done in Practice? Part 1." Presentation at NIST, Gaithersburg, Maryland, August 5, 2010.
- Pont, Piet. "Election through the Internet: Can it be Done in Practice? Part 2." Presentation at NIST, Gaithersburg, Maryland, August 5, 2010.
- Republic and Canton of Geneva, Information Systems Security Unit. *Summary of risk assessment (SAR) by Marti Michel*, January 4, 2008.
- Republic and Canton of Geneva, State Chancellery. *State Council's Report to the Grand Council on the Geneva Electronic Voting Project*. Geneva, Switzerland: July 2007.
- Riera, Andreu and Gerard Cervelló. "Experimentation on Secure Internet Voting in Spain." Presentation at ESF TED workshop, Lochau/Bregenz, Austria, July 8, 2004.
- Rubin, Daniel. "The Security of Remote Online Voting." BS diss., University of Virginia, 2001.

Appendix A: Bibliography

Scytl. *ODBP Project Manual for Kiosk Officials, Version 8.0.*

Paquette, Carol. "Secure Electronic Registration and Voting Experiment (SERVE)." Unpublished presentation, U.S. Election Assistance Commission, Washington, D.C., April 23, 2007.

Stenbjorn, Paul. *D.C. Overseas Digital Vote by Mail Service – An Innovation Effort to Improve Accessibility for UOCAVA Voters.* Washington, D.C.: DCBOEE, September 2010.

U.S. Congress. *Uniformed and Overseas Citizens Absentee Voting Act.* Public Law 99-410. 99th Cong., 2d sess. *U.S. Statutes at Large* 100 (January 1, 1986).

U.S. Congress. *Conference Report to Accompany H.R. 4200.* Washington, D.C., October 8, 2004.

U.S. Election Assistance Commission. *Report to Congress on EAC's Efforts to Establish Guidelines for Remote Electronic Absentee Voting Systems.* Washington, D.C., April 26, 2010.

U.S. Election Assistance Commission. *UOCAVA Pilot Program Testing Requirements.* Washington, D.C., March 24, 2010.

U.S. Election Assistance Commission. *Uniformed and Overseas Citizens Absentee Voting Act Registration and Voting Processes.* Washington D.C.: April 6, 2011.

Victorian Electoral Commission. *The 2010 Victorian State Election Deployment of Electronically Assisted Voting (EAV).* Victoria, Australia: July 2011.

West Virginia Secretary of State. *West Virginia Uniformed Services and Overseas Citizens: Online Voting Pilot Project.* Charleston, West Virginia: January 19, 2011.

Appendix B: Project List

Project:	<i>Alaska</i>
Sponsor:	<i>Democratic National Party</i>
Location:	<i>Alaska</i>
System:	Uncontrolled>Vote Data Return>Web Application
Year	<i>2000</i>

Project:	<i>Arizona 2000</i>
Sponsor:	<i>Arizona Democratic Party</i>
Location:	<i>Arizona</i>
System:	Uncontrolled>Vote Data Return>Web Application
Year	<i>2000</i>

Project:	<i>Arizona 2008/2010</i>
Sponsor:	<i>Arizona Secretary of State's Office</i>
Location:	<i>Arizona</i>
System:	Controlled>Electronic Ballot Return>Web Application/Email/Fax
Year	<i>2008, 2010</i>

Project:	<i>Democrats Abroad</i>
Sponsor:	<i>Democrats Abroad</i>
Location:	<i>United States</i>
System:	Uncontrolled>Vote Data Return>Web Application
Year	<i>2008</i>

Project:	<i>District of Columbia</i>
Sponsor:	<i>DC Board of Elections and Ethics</i>
Location:	<i>District of Columbia</i>
System:	Controlled>Electronic Ballot Return>Web Application
Year	<i>2010</i>

Project:	<i>Honolulu</i>
Sponsor:	<i>City of Honolulu</i>
Location:	<i>Hawaii</i>
System:	Uncontrolled>Vote Data Return>Web Application
Year	<i>2009</i>

Appendix B: Project List

Project:	<i>Michigan</i>
Sponsor:	<i>Michigan Democratic Party</i>
Location:	<i>Michigan</i>
System:	Uncontrolled>Vote Data Return>Web Application/Fax
Year	<i>2004</i>

Project:	<i>ODBP</i>
Sponsor:	<i>Okaloosa County Supervisor of Elections</i>
Location:	<i>Florida</i>
System:	Controlled>Vote Data Return>DRE/Kiosk
Year	<i>2008</i>

Project:	<i>Oregon</i>
Sponsor:	<i>Independent Party of Oregon</i>
Location:	<i>Oregon</i>
System:	Uncontrolled>Vote Data Return>Web Application
Year	<i>2010</i>

Project:	<i>SERVE</i>
Sponsor:	<i>FVAP</i>
Location:	<i>Varying Localities in 5 U.S. States</i>
System:	Uncontrolled>Vote Data Return>Web Application
Year	<i>2004</i>

Project:	<i>West Virginia</i>
Sponsor:	<i>West Virginia Secretary of State</i>
Location:	<i>West Virginia</i>
System:	Uncontrolled>Electronic Ballot Return>Web Application/Email/Fax
Year	<i>2010</i>

Project:	<i>VOI</i>
Sponsor:	<i>FVAP</i>
Location:	<i>Varying Localities in 7 U.S. States</i>
System:	Uncontrolled>Vote Data Return>Web Application
Year	<i>2000</i>

Appendix B: Project List

Project:	<i>Austria</i>
Sponsor:	<i>Federation of Students</i>
Location:	<i>Austria</i>
System:	Uncontrolled>Vote Data Return>Web Application
Year	<i>2009</i>

Project	<i>Estonia</i>
Sponsor:	<i>National Election Commission</i>
Location:	<i>Estonia</i>
System:	Uncontrolled>Vote Data Return>Web Application
Year:	<i>2005, 2007, 2009, 2011</i>

Project	<i>Finland</i>
Sponsor:	<i>Ministry of Justice</i>
Location:	<i>Finland</i>
System:	Controlled>Vote Data Return>DRE/Kiosk
Year:	<i>2008</i>

Project	<i>France</i>
Sponsor:	<i>Multiple Sponsors</i>
Location:	<i>France</i>
System:	<i>Controlled and Uncontrolled forms of Internet voting</i>
Year:	<i>2001, 2002, 2003, 2006, 2009</i>

Project	<i>Netherlands</i>
Sponsor:	<i>Ministry of the Interior and Kingdom Relations</i>
Location:	<i>Netherlands</i>
System:	Uncontrolled>Vote Data>Web Application
Year:	<i>2004, 2006, 2008</i>

Project	<i>Norway</i>
Sponsor:	<i>Ministry of Local Government and Regional Development</i>
Location:	<i>Norway</i>
System:	Uncontrolled>Vote Data Return>Web Application
Year:	<i>2011</i>

Appendix B: Project List

Project	<i>Portugal</i>
Sponsor:	<i>Portuguese Parliament and Government</i>
Location:	<i>Portugal</i>
System:	Uncontrolled>Vote Data Return>Web Application
Year:	<i>2005</i>

Project	<i>Spain</i>
Sponsor:	<i>Oficina de Coordinació Electoral</i>
Location:	<i>Spain</i>
System:	Uncontrolled>Vote Data Return>Web Application
Year:	<i>2003</i>

Project	<i>Geneva</i>
Sponsor:	<i>Geneva State Council</i>
Location:	<i>Geneva, Switzerland</i>
System:	Uncontrolled>Vote Data Return>Web Application
Year:	<i>2004, 2008, 2009, 2010, 2011</i>

Project	<i>Neuchâtel</i>
Sponsor:	<i>The Canton of Neuchâtel</i>
Location:	<i>Neuchâtel, Switzerland</i>
System:	Uncontrolled>Vote Data Return>Web Application
Year:	<i>Annually since 2005</i>

Project	<i>Zurich</i>
Sponsor:	<i>The Canton of Zurich</i>
Location:	<i>Zurich, Switzerland</i>
System:	Uncontrolled>Vote Data Return>Web Application
Year:	<i>2005, 2006, 2008, 2009, 2010, 2011</i>

Project	<i>United Kingdom</i>
Sponsor:	<i>Secretary of State, Ministry of Justice; Electoral Commission</i>
Location:	<i>UK</i>
System:	Controlled and Uncontrolled forms of Internet voting
Year:	<i>2002, 2003, 2007</i>

Appendix B: Project List

Project	<i>Halifax</i>
Sponsor:	<i>Halifax Regional Municipality</i>
Location:	<i>Halifax</i>
System:	Uncontrolled>Vote Data Return>Web Application
Year:	<i>2008</i>

Project	<i>Markham</i>
Sponsor:	<i>Town of Markham</i>
Location:	<i>Markham</i>
System:	Uncontrolled>Vote Data Return>Web Application
Year:	<i>2003, 2006, 2010</i>

Project	<i>Peterborough</i>
Sponsor:	<i>The City of Peterborough</i>
Location:	<i>Peterborough</i>
System:	Uncontrolled>Vote Data Return>Web Application
Year:	<i>2006</i>

Project	<i>AEC</i>
Sponsor:	<i>Joint Standing Committee on Electoral Matters, Australian Electoral Commission, Australian Defence Force</i>
Location:	<i>Australian Defence Force serving in certain locations</i>
System:	Uncontrolled>Vote Data Return>Web Application
Year:	<i>2007</i>

Project	<i>New South Wales</i>
Sponsor:	<i>Premier of New South Wales, Electoral Commissioner</i>
Location:	<i>New South Wales</i>
System:	Uncontrolled>Vote Data Return>Web Application/VOIP
Year:	<i>2011</i>

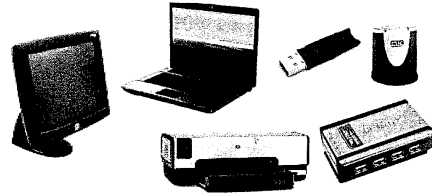
Project	<i>Victoria</i>
Sponsor:	<i>Victorian Election Commission</i>
Location:	<i>Victoria, Australia</i>
System:	Controlled>Vote Data Return>VOIP/DRE/Kiosk
Year:	<i>2010</i>

Appendix C: ODBP Kiosk Equipment

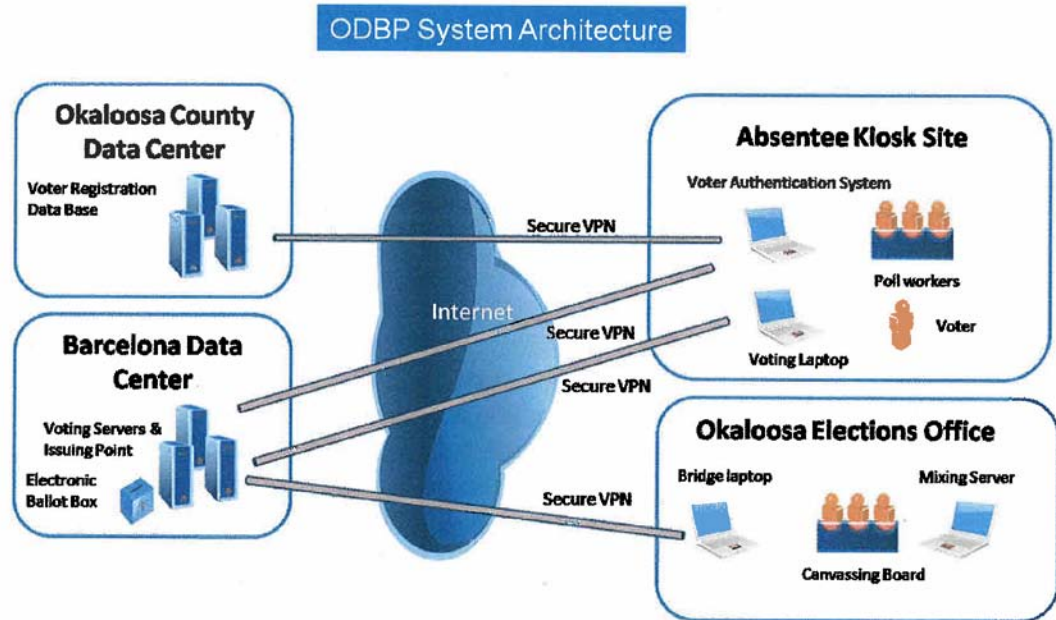
Authentication Laptop



Voting Laptop

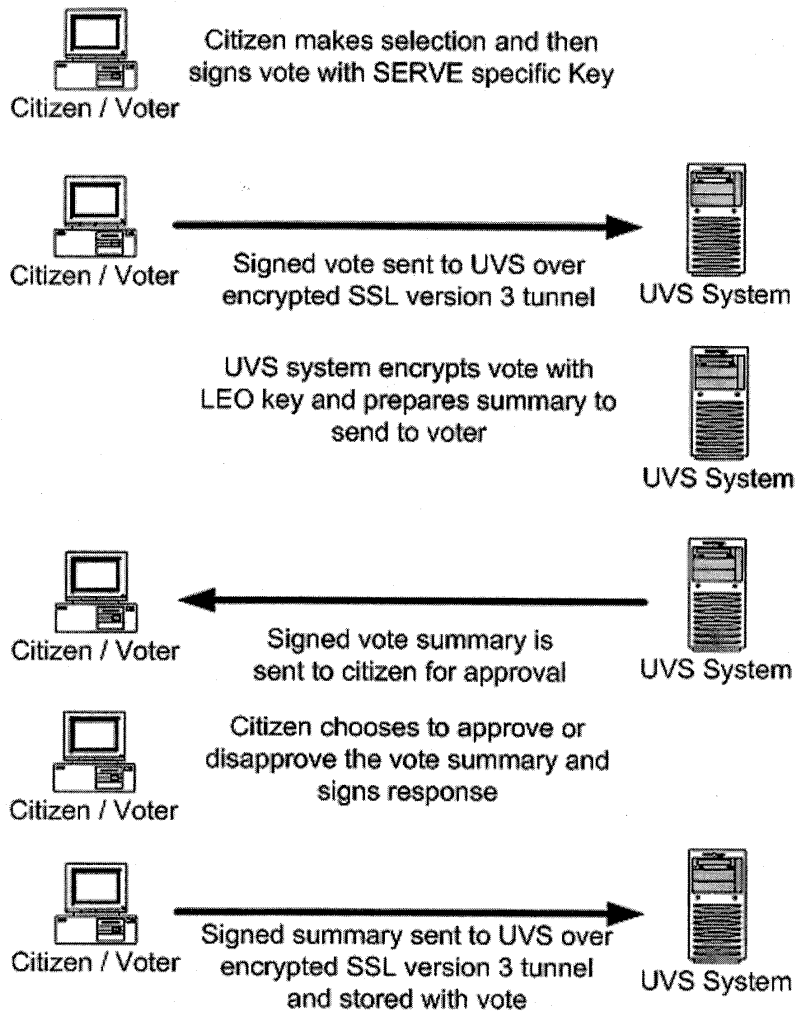


Appendix D: ODBP System Architecture



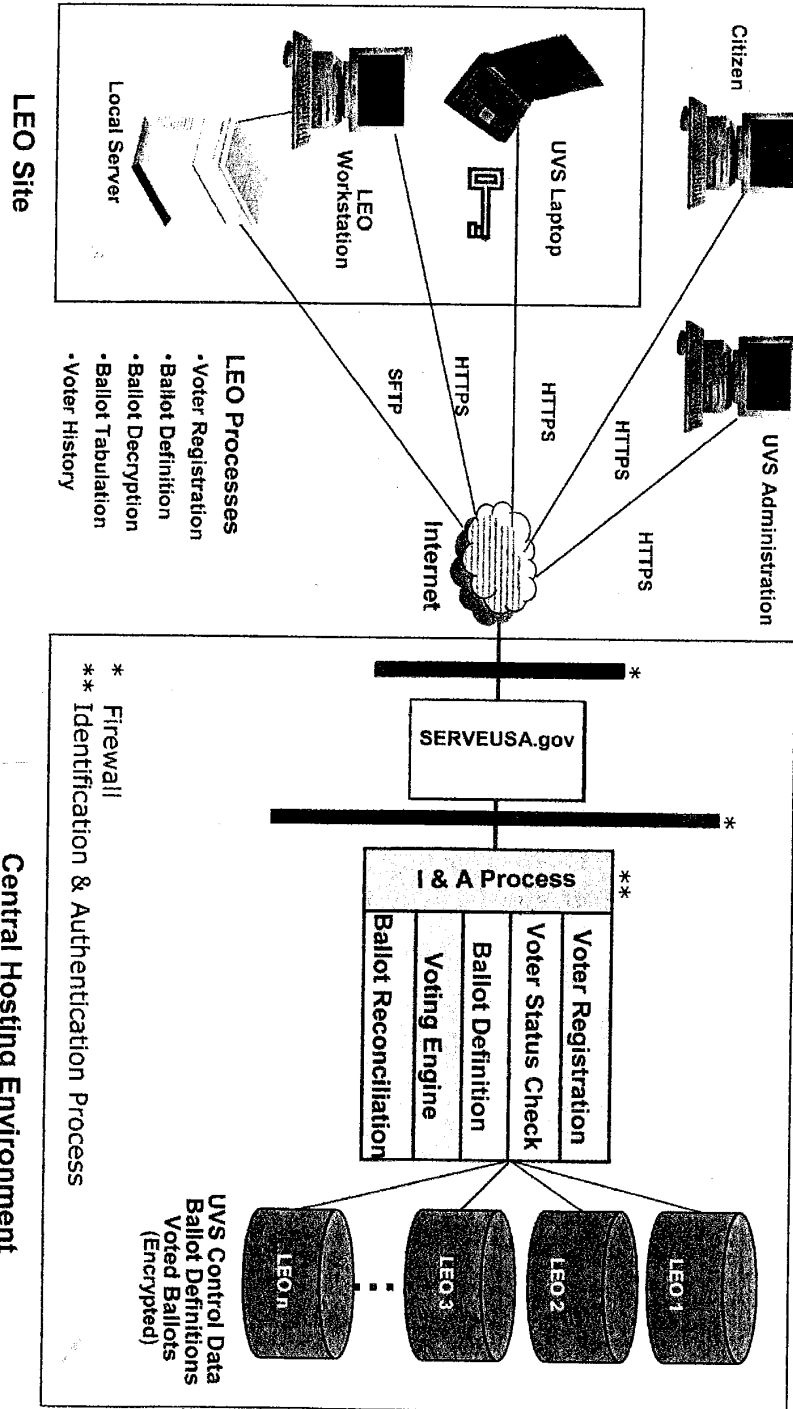
Appendix E: SERVE Voting Protocol

SERVE Voting Action Summary

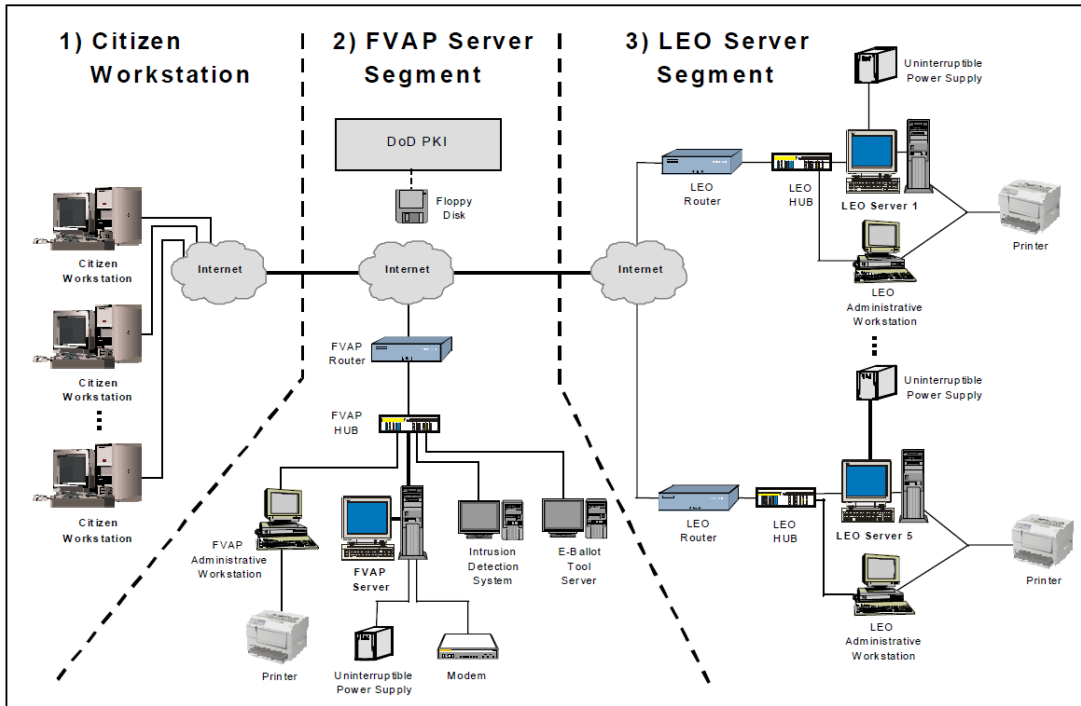


Appendix F: SERVE System Architecture

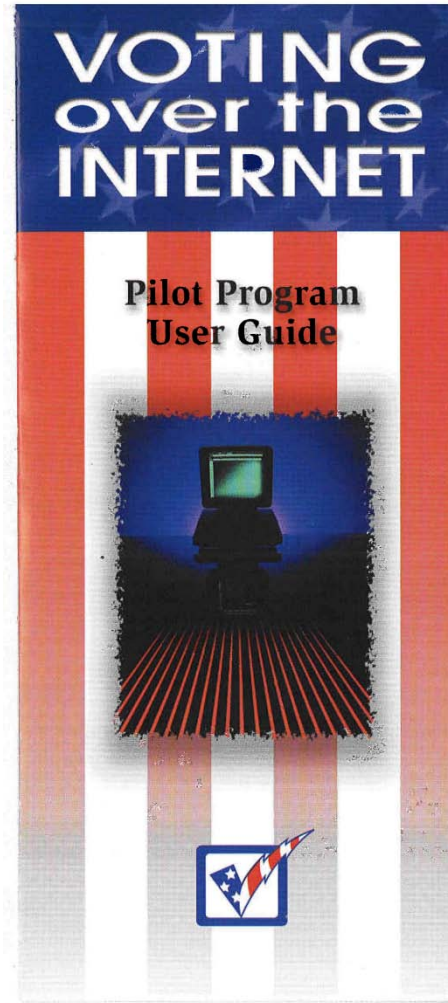
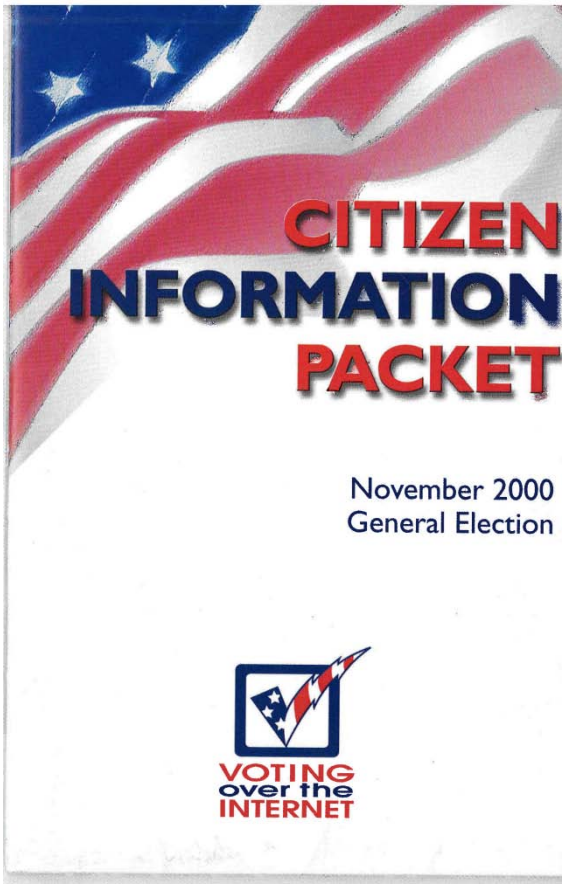
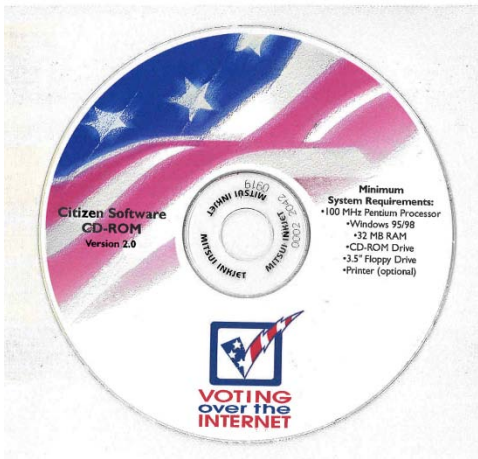
Architecture Overview



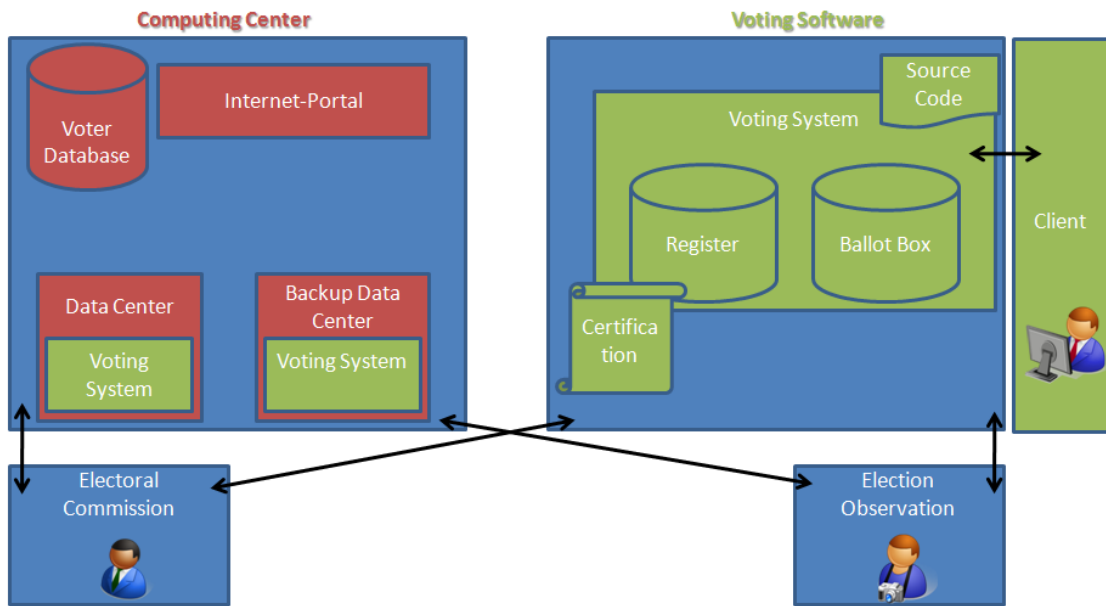
Appendix G: VOI System Diagram



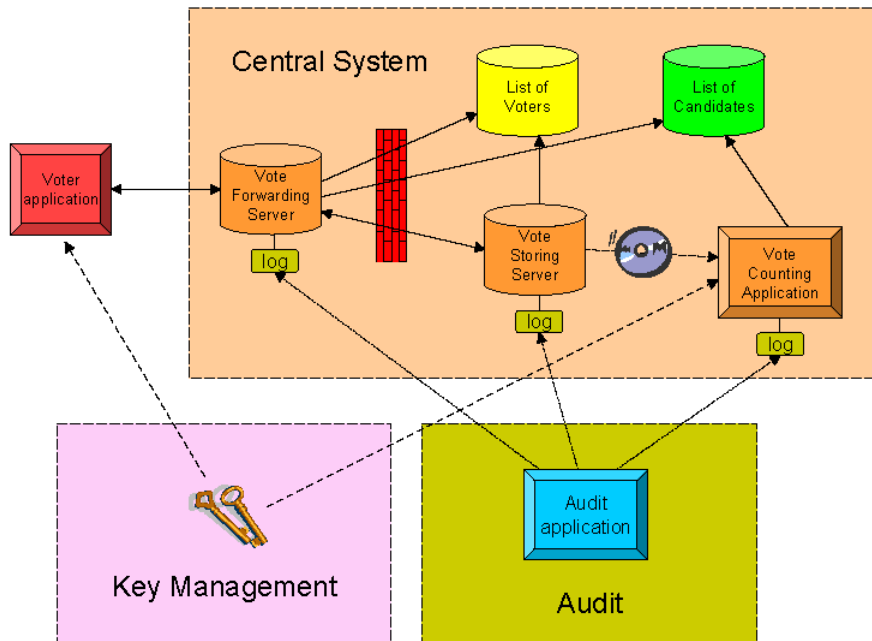
Appendix H: VOI Voter Instructions





Appendix I: Austrian System Architecture



Appendix J: Estonian System Diagram



Appendix K: Netherlands' Voting Card (2004)



Waterschapsverkiezingen Rijnland 2004

stemmen via www.internetstemmen.nl

HIER OPENEN HIER OPENEN

Zo gemakkelijk is stemmen via internet:

- ① Zoek in de kandidatenkrant of op www.rijnland.nl de kandidaat van uw keuze.
- ② Ga naar www.internetstemmen.nl en vul al uw persoonlijke codes in.
- ③ Vervolgens verschijnt uw stembiljet.
- ④ Kies uw kandidaat en bevestig uw keuze.
(Als u voor meer categorieën mag stemmen, volgt u daar eerst informatie over.)
- ⑤ Verstuur uw stemmen door het bevestigen van uw wachtwoord.
(Het stembureau bevestigt de ontvangst van uw stem met een statusverricht. Willt u na de verkiezingen stemcontroles uitvoeren, dan kunt u nu technische informatie over uw stem krijgen en deze bekijken. Stemcontrole kan van 9 t/m 12 oktober op www.rijnland.nl/stemcontrole.)

(Als u voor meer categorieën uw stem mag uitbrengen, verschijnt een nieuw stembiljet. U kiest nu opnieuw een kandidaat en bevestigt uw keuze. Dit herhaalt u voor alle categorieën.)

Uw persoonlijke codes om te stemmen via internet

Deelnemersgroep	>	26	>	162f	>>	msZe
Stemcode	>>	KVMK	>>>	xdx2		
Wachtwoord						

Appendix L: Netherlands' Voting Card (2006)

IV. Bijlage C. Stembescheiden

4

Stemkaart

Voorzijde:



Stemkaart Stemmen via internet

Verkiezing van de leden van de Tweede Kamer der Staten-Generaal

Het internetstembureau is open van zaterdag 18 november 2006 7.30 uur tot woensdag 22 november 2006 21.00 uur
(Nederlandse tijd).

Zo stemt u via internet:

- Ga naar www.internetstembureau.nl
- Vul uw stemcode in. Deze staat in het midden van deze stemkaart.
- Kies de partij van uw keuze of kies 'Blanco' en klik rechtsonder op 'Verder'.
- Kies de kandidaat van uw keuze en klik rechtsonder op 'Verder'.
- Bewestig uw keuze door rechtsonder op de rode knop 'Stem' te klikken.

Uw stemcode:

Stemcode deel 1


Stemcode deel 2

Uw stemcode is strikt persoonlijk en alleen bij uzelf bekend. Bewaar deze tot de stemming op een veilige plaats en vernietig de stemkaart na het uitbrengen van uw stem.

Meer informatie vindt u in de handleiding en op www.kiezenuitbuitenland.nl.
Of bel de helpdesk op +31 70 426 8010






Appendix M: Swiss Election History

 Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

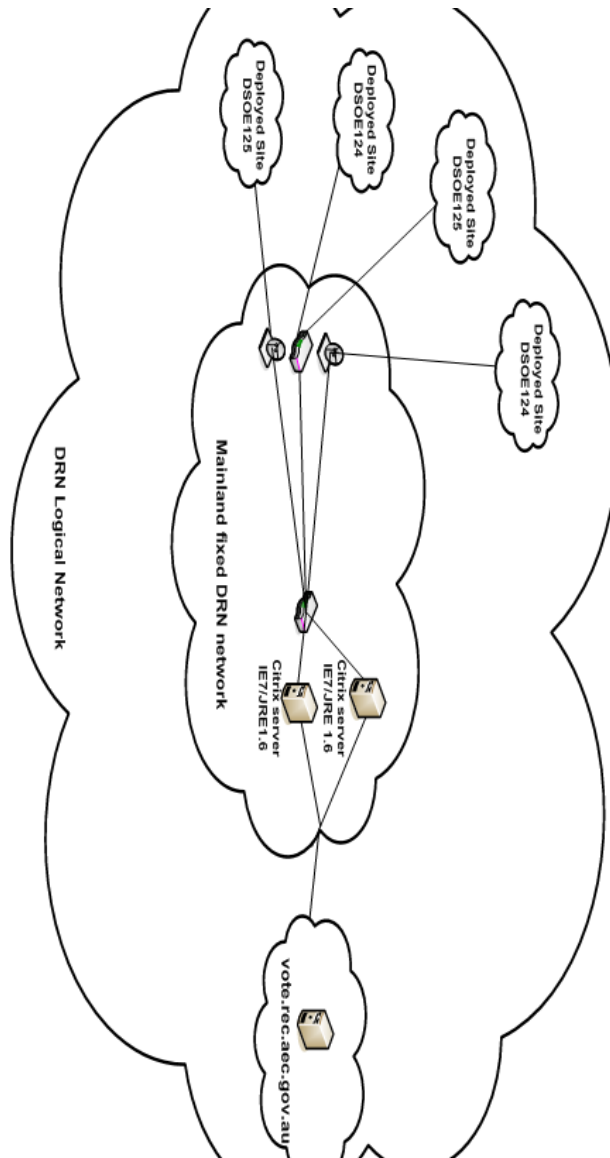
Bundeskanzlei BK
Sektion Politische Rechte

Urnen- gang	Versuche mit Vote électronique (Stufe Bund)											
	NE	GE	ZH	BS	SO	FR	SG	AG	GR	TG	SH	LU
26.09.04		■										
28.11.04		■										
25.09.05	■											
27.11.05	■		■									
26.11.06	■		■									
11.03.07	■		■									
17.06.07	■		■									
24.02.08	■		■									
01.06.08	■		■									
30.11.08	■	■	■									
08.02.09	■	■	■									
17.05.09	■	■	■									
27.09.09	■	■	■									
29.11.09	■	■	■	■								
07.03.10	■	■	■	■	■							
26.09.10	■	■	■	■	■	■						
28.11.10	■	■	■	■	■	■	■	■	■	■	■	■
13.02.11	■	■	■	■	■	■	■	■	■	■	■	■
23.10.11 (Wahlen)				System System			System System	System System	System System			

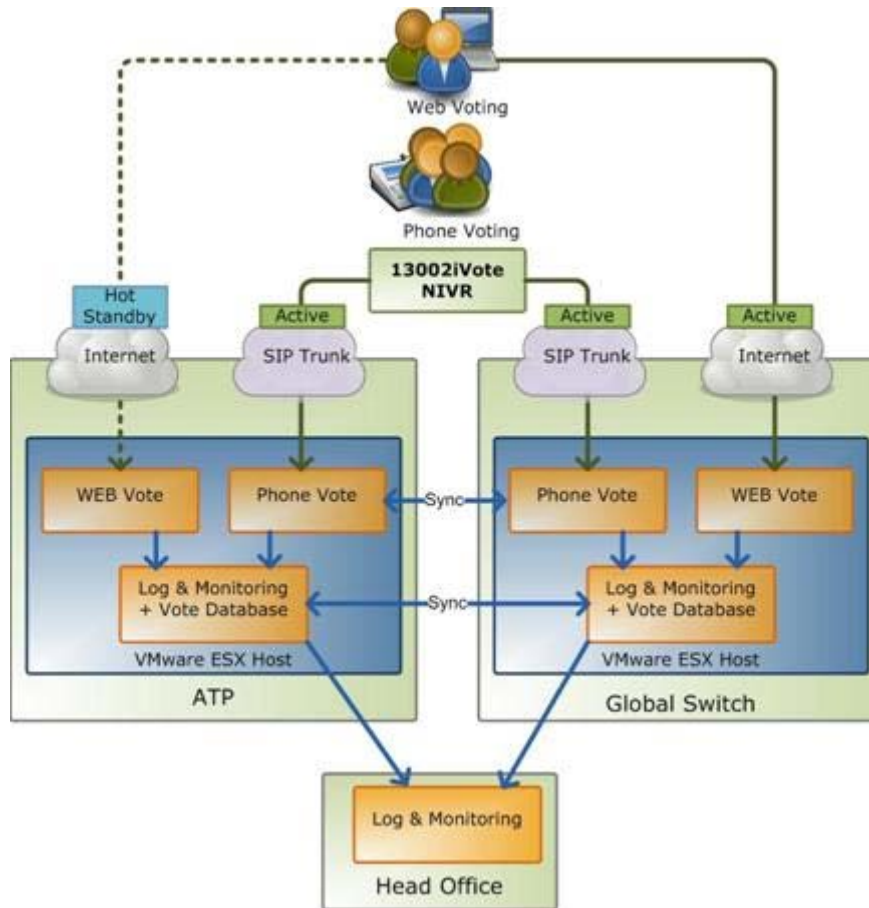
Appendix N: Geneva Voting Card

<p>Chancellerie d'Etat Service des votations et élections</p>  <p>POST TELEMAQUE SA</p>	<p>CAN-COM</p>	<p>CARTE DE VOTE</p>	 <p>Date de naissance complète</p> <table border="1"><tr><td>JOUR</td><td>MOIS</td><td>ANNÉE</td></tr><tr><td> </td><td> </td><td> </td></tr></table> <p>Signature: _____</p> <p>1000072</p> <p>15 mai 2011 VOTATION POPULAIRE Local fictif Electeurs de Test</p> <p>6699-9901</p> <p>PP 1211 Genève 2</p> <p>Monsieur CYBER Citoyen Route Cyberadministration 1 1200 Genève 3</p>	JOUR	MOIS	ANNÉE				<p>A REMPLIR ET SIGNER OBLIGATOIREMENT POUR VOTER PAR CORRESPONDANCE OU AU LOCAL DE VOTE</p> <p>Tout changement d'adresse annoncé à l'office cantonal de la population (OCP) après le 29 MARS 2011 est enregistré mais ne peut figurer sur votre carte de vote, qui atteste de votre domicile à cette date. Une photocopie de cette carte de vote équivalent à l'attestation de résidence officielle délivrée par l'OCP pour 25 F.</p> <p>VOTE PAR INTERNET</p> <p>https://www.evoté.ch/ge</p> <p>Numéro de carte de vote : 1351-5865-2836-4214</p> <p>Code de contrôle : VBP</p> <p>Mot de passe : </p> <p>Empreintes numériques du certificat (certificate fingerprint) : 75:E9:D8:63:F5:DA:13:06:BB:F7:13:36:34:3E:05:42:6C:79:EC:73 OU 1E:78:0D:4E:74:82:ED:A1:1D:86:AC:D7:15:A8:D3:7C</p> <p>Pour être pris en considération, votre vote par internet doit être effectué avant 12h00, le samedi 14 mai 2011</p>
JOUR	MOIS	ANNÉE								

Appendix O: AEC System Architecture



Appendix P: New South Wales System Architecture



Appendix Q: Data Tables

Figure 6-1: System Use Per Year

Project 2000	Usage	Project 2001	Usage	Project 2002	Usage	Project 2003	Usage	Project 2004	Usage
Alaska	1	France	1	UK	5	Spain	1	Michigan	1
Arizona 2000	1			France	1	UK	14	Zurich	1
VOI	1					Markham	1	SERVE	1
						France	1	Netherlands	1
								Geneva	2
Total Usage	3		1		6		17		6

Project 2005	Usage	Project 2006	Usage	Project 2007	Usage	Project 2008	Usage
Estonia	1	Markham	1	Estonia	1	Democrats Abroad	1
Portugal	1	Peterborough	1	UK	5	ODBP	1
Neuchâtel	2	France	1	AEC	1	Finland	1
Zurich	1	Netherlands	1	Neuchâtel	2	Neuchâtel	3
		Neuchâtel	1	Zurich	1	Halifax	1
		Zurich	1			Arizona 2008/2010	1
						Geneva	1
						Zurich	2
Total Usage	5		6		10		11

Appendix Q: Data Tables

Project 2009	Usage	Project 2010	Usage	Project 2011	Usage
Hawaii	1	Oregon	1	Estonia	1
Austria	1	WV 1	1	NSW	1
Estonia	2	WV 2	1	Norway	1
France	1	Markham	1	Geneva	1
Geneva	3	Arizona	1	Neuchâtel	1
Neuchâtel	4	DC	1	Zurich	1
Zurich	4	Geneva	3		
		Neuchâtel	3		
		Zurich	3		
		Victoria	1		
Total Usage	16		16		6

Figure 6-2: System Use by Region

Section	Number of Uses
Canada	7
Europe	77
Oceania	3
USA	12
Total	99

Figure 6-3: System Use by Country

Project	Number of Uses
Australia	3
Austria	1
Canada	7
Estonia	5
Finland	1
France	6
Netherlands	2
Norway	0
Portugal	1
Spain	1
Sweden	0
Switzerland	36
United Kingdom	24
United States	12
Total	99

Figure 6-4: System Use by Project

Project	Number of Uses
Alaska	1
Arizona 2000	1
Arizona 2008/2010	2
Democrats Abroad	1
District of Columbia	0
Hawaii	1
Michigan	1
ODBP	1
Oregon	1
SERVE	0

Appendix Q: Data Tables

West Virginia	2
VOI	1
Austria	1
Estonia	5
Finland	1
France	6
Netherlands	2
Norway	0
Portugal	1
Spain	1
Sweden	0
Geneva	10
Neuchâtel	14
Zurich	12
UK	24
Halifax	2
Markham	3
Peterborough	2
AEC	1
New South Wales	1
Victoria	1
Total Usage	99

Figure 6-4: Voting Environments

Project	Environment
Alaska	Uncontrolled
Arizona 2000	Uncontrolled
Arizona 2008/2010	Uncontrolled
Democrats Abroad	Uncontrolled
District of Columbia	Uncontrolled
Honolulu	Uncontrolled
Michigan	Uncontrolled
ODBP	Controlled
Oregon	Uncontrolled
SERVE	Uncontrolled
West Virginia	Uncontrolled
VOI	Uncontrolled
Austria	Uncontrolled
Estonia	Uncontrolled
Finland	Controlled
France	Excluded
Netherlands	Uncontrolled
Norway	Uncontrolled
Portugal	Uncontrolled
Spain	Uncontrolled
Sweden	Excluded
Geneva	Uncontrolled
Neuchâtel	Uncontrolled
Zurich	Uncontrolled
UK	Excluded
Halifax	Uncontrolled

Appendix Q: Data Tables

Markham	Uncontrolled
Peterborough	Uncontrolled
ADF	Uncontrolled
New South Wales	Uncontrolled
Victoria	Controlled

Endnotes

¹ *Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA)*, Public Law 99-410, 99th Cong., 2d sess. (August 28, 1986).

² U.S. Congress, *Conference Report to Accompany H.R. 4200*, October 8, 2004, page 680.

³ National Science Foundation. *Report of the National Workshop On Internet Voting: Issues and Research Agenda*. (Arlington, Virginia: March, 2001).

⁴ California Internet Voting Task Force, *A Report On the Feasibility of Internet Voting* (Sacramento, California: January, 2000).

⁵ *Ibid.*

⁶ U.S. Election Assistance Commission, *Report to Congress on EAC's Efforts to Establish Guidelines for Remote Electronic Absentee Voting Systems*, Washington, D.C., April 26, 2010.

⁷ Robert E. Kahn and Vinton G. Cerf, *What is the Internet (and What Makes it Work)*, (Washington, D.C.: Internet Policy Institute, December 2009).

⁸ Rebecca Raney, "Voting by the Internet: The Mouse Still Hasn't Roared," *New York Times*, January 30, 2000.

⁹ *Ibid.*

¹⁰ Parisa Baharian, "Internet Voting: Early Efforts," *Online News Hour*, February 7, 2004.

<http://www.pbs.org/newshour/media/interviews/Internetvoting/states.html> (accessed May 19, 2011).

¹¹ R. Michael Alvarez and Thad E. Hall, *Point, Click and Vote: The Future of Internet Voting* (Washington, D.C.: Brookings Institution Press, 2004), page 125.

¹² Parisa Baharian, "Internet Voting: Early Efforts," *Online News Hour*, February 7, 2004.

¹³ *Ibid.*

¹⁴ R. Michael Alvarez and Thad E. Hall, *Point, Click and Vote: The Future of Internet Voting* (Washington, D.C.: Brookings Institution Press, 2004), page 126.

¹⁵ Daniel Rubin, "The Security of Remote Online Voting" (BS diss., University of Virginia, 2001), page 8.

¹⁶ *Ibid.*, page 7.

¹⁷ *Ibid.*, page 8.

¹⁸ R. Michael Alvarez and Thad E. Hall, *Point, Click and Vote: The Future of Internet Voting* (Washington, D.C.: Brookings Institution Press, 2004), page 134.

¹⁹ Williams Matthews, "Can the Net Revive the Vote?" *Federal Computer Week*, entry posted Sep 4, 2000, <http://fcw.com/articles/2000/09/04/can-the-net-revive-the-vote.aspx> (accessed May 19, 2011).

²⁰ Daniel Seligson, "Experts Say Internet Voting Will Have to Wait," *Stateline.org*, entry posted March 6, 2001, <http://www.stateline.org/live/ViewPage.action?siteNodeId=136&languageId=1&contentId=14285> (accessed June 13, 2011).

²¹ Arizona Secretary of State's Office, *Arizona's Military and Overseas System*, by Craig Stender, April 19, 2009, page 1.

²² *Ibid.*

²³ Craig Stender, Interview by Joshua Franklin via telephone, June 13, 2011.

²⁴ Democrats Abroad, *Global Presidential Primary - Results Report* (Washington, D.C.: February 21, 2008 (Revised)).

²⁵ Jody Couser, "Obama Wins Democrats Abroad Global Primary," *Democrats Abroad*, <http://www.democratsabroad.org/article/2008/02/21/obama-wins-democrats-abroad-global-primary> (accessed March 10, 2011).

Endnotes

²⁶ Ibid.

²⁷ Nicole Martinelli, "In an Internet First, Americans Abroad Cast E-Votes in Democratic Primary," *Wired*, entry posted February 5, 2008.

http://www.wired.com/politics/onlinerights/news/2008/02/primary_evote (accessed March 10, 2011).

²⁸ Craig Burton, interview with Jessica Myers, via email, July 31, 2011.

²⁹ Democrats Abroad, *Global Presidential Primary - Results Report* (Washington, D.C.: February 21, 2008 (Revised)).

³⁰ Paul Stenbjorn, *D.C. Overseas Digital Vote by Mail Service - An Innovation Effort to Improve Accessibility for UOCAVA Voters*, (Washington, D.C.: District of Columbia Board of Elections and Ethics, September 2010), page 2.

³¹ Miller Gregory, "D.C. Reality Check – the Opportunities and Challenges of Transparency," *TrustTheVote*, entry posted October 22, 2010, <http://www.trustthevote.org/d-c-reality-check-%e2%80%93-the-opportunities-and-challenges-of-transparency> (accessed June 13, 2011).

³² Ibid.

³³ Alex Halderman, "Hacking the D.C. Internet Voting Pilot" *Freedom to Tinker*, entry posted October 5, 2010, <http://www.freedom-to-tinker.com/blog/jhalderm/hacking-dc-Internet-voting-pilot> (accessed June 13, 2011).

³⁴ Paul Stenbjorn, *D.C. Overseas Digital Vote by Mail Service - An Innovation Effort to Improve Accessibility for UOCAVA Voters*, (Washington, D.C.: District of Columbia Board of Elections and Ethics, September 2010), page 8.

³⁵ Ibid., page 25.

³⁶ Ibid.

³⁷ Ibid.

³⁸ City and County of Honolulu, *Notice of Request for Proposals (RFP-MAY-0900016)* (Honolulu, Hawaii: February 23, 2009), page 24.

³⁹ EveryoneCounts, case study on "Hawaii: The First All-digital Election," <http://www.everyonecounts.com/uploads/pdf/Honolulu%20Case%20Study.pdf> (accessed August 23, 2010).

⁴⁰ Barbara Simons and Justin Moore, "Internet Voting - Not as Easy as You Think," *Verified Voting*, http://votetrustusa.org/index.php?option=com_content&task=view&id=3013&Itemid=26 (accessed June 14, 2011).

⁴¹ City and County of Honolulu, *Notice of Request for Proposals (RFP-MAY-0900016)* (Honolulu, Hawaii: February 23, 2009).

⁴² Ibid, page 22.

⁴³ Ibid.

⁴⁴ City and County of Honolulu, *Proposal Document No. RFP-May-0900016 For On-Line Voting Services for the 2009 Neighborhood Board Elections for the Neighborhood Commission City and County of Honolulu* (Honolulu, Hawaii: March 20, 2009).

⁴⁵ Ibid, page 3.

⁴⁶ Ibid, page 13.

⁴⁷ Ibid, page 10.

⁴⁸ Michigan Democratic Party, press release *John Kerry Wins Michigan Democratic Presidential Caucus*, February 7, 2004.

⁴⁹ Harper West, "Despite Security Concerns, Michigan Democrats Continue Internet Voting," *Verified Voting*, entry posted on February 4, 2004, <http://www.verifiedvotingfoundation.org/article.php?id=1129> (accessed June 14, 2011).

Endnotes

⁵⁰ Ibid.

⁵¹ Wired, "Michigan Dems Vote Online," Wired, <http://www.wired.com/politics/law/news/2004/02/62200> (accessed June 14, 2011).

⁵² Scytl, *ODBP Project Manual for Kiosk Officials* (Version 8.0), Page 44.

⁵³ Florida Department of State, *Florida Administrative Code: Rule 15-2.030* (Tallahassee, Florida: September 13, 2004).

⁵⁴ Operation BRAVO Foundation, *Procedures and System Description for Secure Remote Electronic Transmission of Ballots for Overseas Civilian and Military Voters* (Okaloosa, FL: Operation Bravo Foundation; June 19, 2008).

⁵⁵ Florida Department of State, *Provisional Qualification Test Report: Scytl Release 1.0, Version 1* (Tallahassee, FL: Florida Department of State; September 23, 2008).

⁵⁶ Operation BRAVO Foundation, *Procedures and System Description for Secure Remote Electronic Transmission of Ballots for Overseas Civilian and Military Voters* (Okaloosa, FL: Operation Bravo Foundation; June 19, 2008).

⁵⁷ Clarkson, Michael, Brian Hay, Meador Inge, Abhi Shelat, David Wagner, Alec Yasinsac, *Software Review and Security Analysis of Scytl Remote Voting Software* (Tallahassee, FL: Florida State University's (FSU) Security and Assurance in Information Technology (SAIT) Laboratory; September 19, 2008).

⁵⁸ Operation BRAVO Foundation, *Procedures and System Description for Secure Remote Electronic Transmission of Ballots for Overseas Civilian and Military Voters* (Okaloosa, FL: Operation Bravo Foundation; June 19, 2008).

⁵⁹ Sal Peralta, Secretary of the Independent Party of Oregon, interview by Joshua Franklin via telephone, October 7, 2010.

⁶⁰ Ibid.

⁶¹ Kari Chisholm, "The Independent Party Primary Election" BlueOregon, entry posted July 12, 2010, <http://www.blueoregon.com/2010/07/independent-party-primary-election/> (accessed June 14, 2011).

⁶² Sal Peralta, Secretary of the Independent Party of Oregon, interview by Joshua Franklin via telephone, October 7, 2010.

⁶³ Ibid.

⁶⁴ Ibid.

⁶⁵ Dr. David Jefferson, Dr. Aviel Rubin, Dr. Barbara Simons, and Dr. David Wagner, *A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)* (January 21, 2004).

⁶⁶ Carol Paquette, "Secure Electronic Registration and Voting Experiment (SERVE)," (presentation, U.S. Election Assistance Commission, Washington, DC, April 23, 2007).

⁶⁷ SERVE Program Documents, *SERVE Voting Action Summary*.

⁶⁸ Ibid.

⁶⁹ SERVE Program documents, *SERVE Digital Signature Subscriber Agreement*.

⁷⁰ SERVE Program documents, *SERVE Requirements Document*.

⁷¹ Department of Defense, Federal Voting Assistance Program, *Voting Over the Internet Pilot Project Assessment Report* (Washington Headquarters, Washington, DC, June 2001).

⁷² Carol Paquette, interview by Josh Franklin, Washington, DC, July 22, 2011.

⁷³ SERVE Program Documents, *Memorandum of Understanding*.

⁷⁴ Ibid.

⁷⁵ West Virginia Secretary of State, legislative report *West Virginia Uniformed Services and Overseas Citizen: Online Voting Pilot Project* (Charleston, West Virginia: January 19, 2011), page 5.

Endnotes

⁷⁶ Jake Glance, "West Virginia's Internet Voting Pilot Program Featured in Pew Center Newsletter," West Virginia Secretary of State Website, entry posted May 21, 2010, <http://www.sos.wv.gov/news/topics/elections-candidates/Pages/WestVirginia%27sInternetVotingPilotProgramFeaturedInPewCenterNewsletter.aspx> (accessed June 14, 2011).

⁷⁷ Ibid.

⁷⁸ West Virginia Secretary of State, legislative report *West Virginia Uniformed Services and Overseas Citizen: Online Voting Pilot Project* (Charleston, West Virginia: January 19, 2011), Page 2.

⁷⁹ Ibid, Page 1.

⁸⁰ Jackie Harris, Policy Director, West Virginia Secretary of State, interview by Joshua Franklin via telephone, January 19, 2011.

⁸¹ West Virginia Secretary of State. Legislative Report - West Virginia Uniformed Services and Overseas Citizen: Online Voting Pilot Project. West Virginia, Page 4. January 19, 2011.

⁸² Ibid.

⁸³ Ibid.

⁸⁴ West Virginia Secretary of State, legislative report *West Virginia Uniformed Services and Overseas Citizen: Online Voting Pilot Project* (Charleston, West Virginia: January 19, 2011), Page 8.

⁸⁵ Ibid., page 9.

⁸⁶ Ibid., page 13.

⁸⁷ Ibid, page 1.

⁸⁸ Department of Defense, Federal Voting Assistance Program, *Voting Over the Internet Pilot Project Assessment Report* (Washington Headquarters, Washington, DC, June 2001), page 1.

⁸⁹ Carol Paquette, interview with Josh Franklin, Washington, DC, July 22, 2011.

⁹⁰ Ibid.

⁹¹ FVAP, "VOI Citizen Guide November 2000 General Election" distributed as part of the *Citizen Information Packet*.

⁹² Ibid.

⁹³ Department of Defense, Federal Voting Assistance Program, *Voting Over the Internet Pilot Project Assessment Report* (Washington Headquarters, Washington, DC, June 2001).

⁹⁴ Ibid.

⁹⁵ Federal Voting Assistance Program, *Voting Over the Internet System Security Authorization Agreement* (FVAP, Washington, DC, March 2001), Section 4.

⁹⁶ Department of Defense, Federal Voting Assistance Program, *Voting Over the Internet Pilot Project Assessment Report* (Washington Headquarters, Washington, DC, June 2001).

⁹⁷ FVAP, *Memorandum of Agreement between the Federal Voting Assistance Program and the States of Florida, Missouri, South Carolina, Texas and Utah*.

⁹⁸ Ibid.

⁹⁹ Robert Krimmer, interview by Joshua Franklin via email. January 3, 2011.

¹⁰⁰ Robert Krimmer, Andreas Ehringfeld, and Markus Traxl, "The Use of E-Voting in the Federation of Students' Elections 2009," (paper presented at the EVOTE2010 conference, Lochau/Bregenz, Austria, July 22, 2010).

¹⁰¹ Robert Krimmer and Gregor Wenda, "Electronic Voting in Austria: Experiences and Challenges," (presentation in Oslo, Norway, March 19, 2010).

¹⁰² Robert Krimmer, "Implementing Electronic Voting: The Austrian Experience," (lecture given at TED summer school, Varenna, Italy, September 7-13, 2003). <http://www.sal.hut.fi/TED/slides/Krimmer.ppt>

Endnotes

- ¹⁰³ Bundesministerium für Wissenschaft und Forschung, *E-Voting bei den Hochschülerinnen- und Hochschüler-schaftswahlen 2009* (Vienna, Austria: March 29, 2010).
- ¹⁰⁴ Robert Krimmer, interview by Joshua Franklin via email. January 3, 2011.
- ¹⁰⁵ Ibid.
- ¹⁰⁶ Ibid.
- ¹⁰⁷ Robert Krimmer and Gregor Wenda, "Electronic Voting in Austria: Experiences and Challenges," (presentation in Oslo, Norway, March 19, 2010).
- ¹⁰⁸ Robert Krimmer, Andreas Ehringfeld, and Markus Traxl, "The Use of E-Voting in the Federation of Students' Elections 2009," (paper presented at the EVOTE2010 conference, Lochau/Bregenz, Austria, July 22, 2010).
- ¹⁰⁹ Jordi Puiggali, Interview by Joshua Franklin via email, March 2, 2011.
- ¹¹⁰ Robert Krimmer, Andreas Ehringfeld, and Markus Traxl, "The Use of E-Voting in the Federation of Students' Elections 2009," (paper presented at the EVOTE2010 conference, Lochau/Bregenz, Austria, July 22, 2010).
- ¹¹¹ Jordi Puiggali, Interview by Joshua Franklin via email, March 2, 2011.
- ¹¹² Robert Krimmer, Andreas Ehringfeld, and Markus Traxl, "The Use of E-Voting in the Federation of Students' Elections 2009," (paper presented at the EVOTE2010 conference, Lochau/Bregenz, Austria, July 22, 2010).
- ¹¹³ Robert Krimmer and Gregor Wenda, "Electronic Voting in Austria: Experiences and Challenges," (presentation in Oslo, Norway, March 19, 2010).
- ¹¹⁴ Andreas Ehringfeld, Larissa Naber, Thomas Grechenig, Robert Krimmer, Markus Traxl, Gerald Fischer. "Analysis of Recommendation Rec(2004)11 Based on the Experiences of Specific Attacks Against the First Legally Binding Implementation of E-Voting in Austria," (paper presented at the EVOTE2010 conference, Lochau/Bregenz, Austria, July 22, 2010).
- ¹¹⁵ Tarvi Martens, interview by Joshua Franklin via email, received July 6, 2011.
- ¹¹⁶ National Electoral Committee (Estonia), *E-Voting Conception Security: Analysis and Measures* (Tallinn, Estonia: December 15, 2003), page 16.
- ¹¹⁷ Katholieke Universiteit Leuven, *BeVoting Study of Electronic Voting Systems* (Leuven, Belgium: April 15, 2007), page 159.
- ¹¹⁸ Ibid.
- ¹¹⁹ Canada-Europe Transatlantic Dialogue, *A Comparative Assessment of Electronic Voting* (Ottawa, ON: February 2010), page 34.
- ¹²⁰ Estonian National Electoral Committee, "Statistics about Internet Voting in Estonia," Estonian National Electoral Committee website, <http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics> (accessed August 9, 2011).
- ¹²¹ Ibid.
- ¹²² Tarvi Martens, email message to Josh Franklin, "Internet Voting in Estonia (Slide 6)," received July 1, 2011.
- ¹²³ National Electoral Committee (Estonia), *Internet Voting in Estonia* (Tallinn, Estonia: 2007).
- ¹²⁴ Katholieke Universiteit Leuven, et al, *BeVoting Study of Electronic Voting Systems* (Leuven, Belgium: April 15, 2007), Page 20-21.
- ¹²⁵ Canada-Europe Transatlantic Dialogue, *A Comparative Assessment of Electronic Voting* (Ottawa, ON: February 2010), Page 34.
- ¹²⁶ Ibid.
- ¹²⁷ National Electoral Committee (Estonia), *E-Voting Conception Security: Analysis and Measures* (Tallinn, Estonia: December 15, 2003), page 4.

Endnotes

- ¹²⁸ Ibid., page 18 - 35.
- ¹²⁹ Ibid., page 18.
- ¹³⁰ Ibid., page 37.
- ¹³¹ Ibid., page 34 - 35.
- ¹³² Ibid., page 38.
- ¹³³ Jordi Puiggali, interview by Joshua Franklin via email, March 2, 2011.
- ¹³⁴ Ministry of Justice (Finland), *Electronic Voting Pilot in the 2008 Municipal Elections* (Helsinki, Finland, November 4, 2010), page 2.
- ¹³⁵ Jussi Aaltonen, "eVoting 2008: Statistics," (presentation at Ministry of Justice, Finland).
- ¹³⁶ Ministry of Justice (Finland), *Electronic Voting Pilot in the 2008 Municipal Elections* (Helsinki, Finland, November 4, 2010), page 1.
- ¹³⁷ Ibid.
- ¹³⁸ Jordi Puiggali, interview by Joshua Franklin via email, March 2, 2011.
- ¹³⁹ Ibid.
- ¹⁴⁰ Ministry of Justice (Finland), "The voting process - Electronic Voting 2008," Ministry of Justice website, http://www.vaalit.fi/sahkoinenaanestaminen/en/aanestyksen_kulku.html (accessed June 15, 2011).
- ¹⁴¹ Ministry of Justice (Finland), *Electronic Voting Pilot in the 2008 Municipal Elections* (Helsinki, Finland, November 4, 2010), page 3.
- ¹⁴² Ibid.
- ¹⁴³ Ibid., page 5.
- ¹⁴⁴ Ibid., page 5.
- ¹⁴⁵ Ibid.
- ¹⁴⁶ Ibid.
- ¹⁴⁷ Jordi Puiggali, interview by Joshua Franklin via email, March 2, 2011.
- ¹⁴⁸ Ministry of Justice (Finland), "Only supervised voting allowed - Electronic Voting 2008," Ministry of Justice Website, <http://www.vaalit.fi/sahkoinenaanestaminen/en/valvotusti.html> (accessed June 15, 2011).
- ¹⁴⁹ Ministry of Justice (Finland), "Why has Internet voting not been arranged?- Electronic Voting 2008," Ministry of Justice website, <http://www.vaalit.fi/sahkoinenaanestaminen/en/ukk/ukk20.html> (accessed June 15, 2011).
- ¹⁵⁰ Ministry of Science, Technology and Higher Education (Portugal), "Electronic Voting Experiments in Political Elections around the World," Knowledge Science Agency website, http://www.english.umic.pt/index.php?option=com_content&task=view&id=3113&itemid (accessed March 16, 2011).
- ¹⁵¹ Ibid.
- ¹⁵² Ibid.
- ¹⁵³ Ibid.
- ¹⁵⁴ Jordi Puiggali, interview by Joshua Franklin via email, March 2, 2011.
- ¹⁵⁵ Ibid.
- ¹⁵⁶ Ibid.
- ¹⁵⁷ Ibid.
- ¹⁵⁸ Ibid.
- ¹⁵⁹ Ibid.
- ¹⁶⁰ Ibid.

Endnotes

- ¹⁶¹ Ibid.
- ¹⁶² Ibid.
- ¹⁶³ Ibid.
- ¹⁶⁴ Ibid.
- ¹⁶⁵ Ibid.
- ¹⁶⁶ Ibid.
- ¹⁶⁷ Ibid.
- ¹⁶⁸ Office for Democratic Institutions and Human Right, *OSCE/ODIHR Election Assessment Mission Report: The Netherlands Parliamentary Elections 22 November 2006* (Vienna, Austria: March 12, 2007), page 14.
- ¹⁶⁹ Susanne Caarls, interview with Josh Franklin, via email, August 4, 2011.
- ¹⁷⁰ Office for Democratic Institutions and Human Right, *OSCE/ODIHR Election Assessment Mission Report: The Netherlands Parliamentary Elections 22 November 2006* (Vienna, Austria: March 12, 2007), page 14.
- ¹⁷¹ Susanne Caarls, interview with Josh Franklin, via email, August 4, 2011.
- ¹⁷² Ibid.
- ¹⁷³ Piet Pont, *RIES Facts and Features Sheet*, created July 28, 2010, http://csrc.nist.gov/groups/ST/UOCAVA/2010/PositionPapers/PIET_PONT_RIES_UOCAVA.pdf (accessed June 6, 2011).
- ¹⁷⁴ Susanne Caarls, interview with Josh Franklin, via email, August 4, 2011.
- ¹⁷⁵ Ibid.
- ¹⁷⁶ Ibid.
- ¹⁷⁷ Ibid.
- ¹⁷⁸ Ibid.
- ¹⁷⁹ Ibid.
- ¹⁸⁰ Piet Pont, "Elections through the Internet: Can It Be Done in Practice? Part 2" (presentation at NIST, Gaithersburg, Maryland, August 5, 2010).
- ¹⁸¹ Piet Pont, "Elections through the Internet: Can It Be Done in Practice? Part 2" (presentation at NIST, Gaithersburg, Maryland, August 5, 2010).
- ¹⁸² "Office for Democratic Institutions and Human Right, *OSCE/ODIHR Election Assessment Mission Report: The Netherlands Parliamentary Elections 22 November 2006* (Vienna, Austria: March 12, 2007).
- ¹⁸³ Ibid.
- ¹⁸⁴ Ibid.
- ¹⁸⁵ Susanne Caarls, interview with Josh Franklin, via email, August 4, 2011.
- ¹⁸⁶ Ibid.
- ¹⁸⁷ Susanne Caarls, interview with Josh Franklin, via email, August 4, 2011.
- ¹⁸⁸ Ministry of Local Government and Regional Development (Norway), *E-vote 2011 System Architecture Overview, Interfaces and Deployment V 1.5* (Oslo, Norway: April 25, 2011), page 23.
- ¹⁸⁹ Ministry of Local Government and Regional Development (Norway), *E-vote 2011 System Architecture – eVote V 1.3* (Oslo, Norway: June 13, 2011), page 41.
- ¹⁹⁰ Ministry of Local Government and Regional Development (Norway), *Electronic voting– challenges and opportunities* (Oslo, Norway: 2006), page 1.
- ¹⁹¹ Ibid., page 6.
- ¹⁹² Ibid., page 133.
- ¹⁹³ Ibid., page 128.

Endnotes

¹⁹⁴ Ministry of Local Government and Regional Development (Norway), "11 Municipalities to Try Out E-Voting in 2011," Ministry of Local Government and Regional Development website, <http://www.regjeringen.no/en/dep/krd/pressesenter/pressemeldinger/2010/11-kommunar-far-prove-e-val-i-2011.html?id=591610> (accessed June 9, 2011).

¹⁹⁵ Henrik Nore, "Open Source Remote Electronic Voting in Norway" (presentation at the OSCE Chairmanship Seminar, Working Session III, Vienna, Austria, September 17, 2010).

¹⁹⁶ Ministry of Local Government and Regional Development (Norway), "Evote 2011 Project," Ministry of Local Government and Regional Development website, <http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project.html?id=597658> (accessed June 9, 2011).

¹⁹⁷ Kristian Gjøsteen, "Analysis of an Internet Voting Protocol," *Cryptology ePrint Archive* (July 7, 2010), <http://eprint.iacr.org/2010/380.pdf> (accessed June 9, 2011).

¹⁹⁸ Ibid.

¹⁹⁹ Ibid.

²⁰⁰ Ministry of Local Government and Regional Development (Norway), *E-vote 2011: Election system with solution for electronic voting, Norway 2011* (Oslo, Norway: 2009).

²⁰¹ Ministry of Local Government and Regional Development (Norway), *E-vote 2011: System Requirements Specification* (Oslo, Norway: September 10, 2009).

²⁰² Ministry of Local Government and Regional Development (Norway), *e-Vote 2011 Security Objectives* (Oslo, Norway: September 25, 2009), page 11.

²⁰³ Ministry of Local Government and Regional Development (Norway), *e-Vote 2011 Security Objectives* (Oslo, Norway: September 25, 2009).

²⁰⁴ Ibid.

²⁰⁵ Ibid.

²⁰⁶ João Falcão e Cunha, Mário Jorge Leitão, João Pascoal Faria, Miguel Pimenta Montiero, and Maria Antónia Carravilla, "A Methodology for Auditing e-Voting Processes and Systems used at the Elections for the Portuguese Parliament," *Electronic Voting 2006: Lecture Notes in Informatics*, by Robert Krimmer (ed.), August 2-4, 2006, page 146.

²⁰⁷ Ibid., page 152.

²⁰⁸ Ibid., page 152-153.

²⁰⁹ Andreu Riera and Gerard Cervelló, "Experimentation on Secure Internet Voting in Spain," (presented ESF TED workshop, Lochau/Bregenz, Austria, July 8, 2004), Page 95.

²¹⁰ Ibid, page 91.

²¹¹ Ibid.

²¹² Ibid, page 94.

²¹³ Ibid.

²¹⁴ Ibid, page 92.

²¹⁵ Ibid, page 91.

²¹⁶ Ibid, page 92.

²¹⁷ Ministry of Justice, Election Technique Commission (Sweden), excerpts from *Technology and Administration in Election Procedure Final Report from the Election Technique 2000 Commission* (Stockholm, Sweden: 2000), page 1.

²¹⁸ Ibid., page 8.

²¹⁹ Ibid., page 8-11.

Endnotes

- ²²⁰ Ministry of Justice, Election Technique Commission (Sweden), excerpts from *Technology and Administration in Election Procedure Final Report from the Election Technique 2000 Commission* (Stockholm, Sweden: 2000).
- ²²¹ Tomas Ohlin and Markus Hällgren, "Internet Voting in Practice: The Case of the Umeå Student Union," *e-Service Journal*: (Fall 2002), page 36.
- ²²² Ibid.
- ²²³ Ibid., page 55.
- ²²⁴ Ministry of Justice, Election Technique Commission (Sweden), excerpts from *Technology and Administration in Election Procedure Final Report from the Election Technique 2000 Commission* (Stockholm, Sweden: 2000), page 2.
- ²²⁵ Ibid.
- ²²⁶ Ibid.
- ²²⁷ Katholieke Universiteit Leuven, et al, *BeVoting Study of Electronic Voting Systems* (Leuven, Belgium: April 15, 2007), page 40.
- ²²⁸ Daniel Munster, interview by Joshua Franklin, Zurich, Switzerland, July 23, 2010.
- ²²⁹ Ibid.
- ²³⁰ Ibid.
- ²³¹ Ibid.
- ²³² Republic and Canton of Geneva, State Chancellery, *State Council's Report to the Grand Council on the Geneva Electronic Voting Project* (Geneva, Switzerland: July 2007), page 15.
- ²³³ Ibid., page 7.
- ²³⁴ Ibid., page 10.
- ²³⁵ Ibid.
- ²³⁶ Ibid., Page 7.
- ²³⁷ Michel Chevallier, interview by Joshua Franklin, Geneva, Switzerland, July 24, 2010.
- ²³⁸ Republic and Canton of Geneva, State Chancellery, *State Council's Report to the Grand Council on the Geneva electronic voting project* (Geneva, Switzerland: July 2007), page 15.
- ²³⁹ Michel Chevallier, *Internet Voting: Situation Perspectives and Issues (Slide 20)*, Geneva State Chancellery, received July 24, 2010.
- ²⁴⁰ Michel Chevallier, interview by Joshua Franklin, Geneva, Switzerland, July 24, 2010.
- ²⁴¹ Republic and Canton of Geneva, State Chancellery, *State Council's Report to the Grand Council on the Geneva electronic voting project* (Geneva, Switzerland: July 2007), page 47.
- ²⁴² Ibid.
- ²⁴³ Ibid, page 4.
- ²⁴⁴ Michel Chevallier, *e-voting Certification Project, Voting via the Internet (Slide 8)*, Geneva State Chancellery, November 11, 2008.
- ²⁴⁵ Marti Michel, *Summary of Risk Assessment (SAR)*, Republic and Canton of Geneva, Information systems security unit, January 4, 2008.
- ²⁴⁶ Ibid., page 7.
- ²⁴⁷ Republic and Canton of Geneva, State Chancellery, *State Council's Report to the Grand Council on the Geneva electronic voting project* (Geneva, Switzerland: July 2007), page 15.
- ²⁴⁸ Jordi Puiggali, interview by Joshua Franklin via email, March 2, 2011.
- ²⁴⁹ Gerard Cervelló, "The E-Participation Project of Neuchâtel," *European Journal of ePractice* (March 2009), page 1.
- ²⁵⁰ Jordi Puiggali, interview by Joshua Franklin via email, March 2, 2011.

Endnotes

²⁵¹ Ibid.

²⁵² Gerard Cervelló, "The E-Participation Project of Neuchâtel," *European Journal of ePractice* (March 2009), page 3.

²⁵³ Jordi Puiggali, interview by Joshua Franklin via email, March 2, 2011.

²⁵⁴ Ibid.

²⁵⁵ Jan Gerlach and Urs Gasser, "Three Case Studies from Switzerland: E-Voting," *Internet and Democracy Case Study Series* (March 2009), http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Gerlach-Gasser_SwissCases_Evoting.pdf (accessed May 25, 2011), page 6.

²⁵⁶ Ibid., page 7.

²⁵⁷ Giampiero Beroggi, "Secure and Easy Internet Voting," *Computer* (IEEE Magazine), February 2008, page 53.

²⁵⁸ Ibid.

²⁵⁹ Giampiero Beroggi, "E-Voting through the Internet and with Mobile Phones," United Nations Public Administration Network, <http://unpan1.un.org/intradoc/groups/public/documents/unpan/unpan030950.pdf> (accessed May 25, 2011), page 2.

²⁶⁰ Ibid., page 3.

²⁶¹ Ibid.

²⁶² Electoral Commission (UK), "The Electoral Commission Website," Electoral Commission United Kingdom, <http://www.electoralcommission.org.uk/> (accessed May 2011).

²⁶³ Electoral Commission (UK), *Modernising Elections: A Strategic Evaluation of the 2002 Electoral Pilot Schemes* (London, England: August 2002), page 40.

²⁶⁴ Ibid., page 21.

²⁶⁵ Ibid., page 40.

²⁶⁶ Ibid.

²⁶⁷ Ibid., page 41.

²⁶⁸ Australian Electoral Commission, *eVolution not Revolution: Electronic Voting Status Report* (Parkes ACT, Australia: September 2002), page 9.

²⁶⁹ Ibid., pages 8, 10-11.

²⁷⁰ Ibid., pages 7-8, 11.

²⁷¹ Ibid., pages 6-7, 9, 11.

²⁷² Ibid., page 9.

²⁷³ Ibid., pages 8, 10.

²⁷⁴ Electoral Commission (UK), *Modernising Elections: A Strategic Evaluation of the 2002 Electoral Pilot Schemes* (London, England: August 2002), page 44.

²⁷⁵ Ibid., pages 74-79.

²⁷⁶ Electoral Commission (UK), *The Shape of Elections to Come: A Strategic Evaluation of the 2003 Electoral Pilot Schemes* (London, England: July 2003), pages 50 & 63.

²⁷⁷ Ibid., page 51.

²⁷⁸ Ibid.

²⁷⁹ Ibid.

²⁸⁰ Ibid.

²⁸¹ Ibid.

²⁸² Ibid.

Endnotes

- ²⁸³ Ibid., pages s 52-53.
- ²⁸⁴ Ibid., page 53.
- ²⁸⁵ Ibid., page 65.
- ²⁸⁶ Ibid., page 64.
- ²⁸⁷ Ibid., page 54.
- ²⁸⁸ Ibid., pages s 54-59.
- ²⁸⁹ Electoral Commission (UK), *Electronic Voting: May 2007 Electoral Pilot Schemes* (London, England: May 2007), page 2.
- ²⁹⁰ Ibid.
- ²⁹¹ Ibid., page 3.
- ²⁹² Ibid., page 10.
- ²⁹³ Canada-Europe Transatlantic Dialogue, *A Comparative Assessment of Electronic Voting* (Ottawa, ON: February 2010), page 24.
- ²⁹⁴ Ibid.
- ²⁹⁵ Ibid., pages 19-21.
- ²⁹⁶ Cathy Mellett, interview by Joshua Franklin via email, July 12, 2011.
- ²⁹⁷ Ibid.
- ²⁹⁸ Ibid.
- ²⁹⁹ Ibid.
- ³⁰⁰ Cathy Mellett, "HRM's Experience with Electronic Voting" (Lecture, Policy Workshop, "Internet Voting: What can Canada Learn?," Carleton University, January 26, 2010).
- ³⁰¹ Cathy Mellett, interview by Joshua Franklin via email, July 12, 2011.
- ³⁰² Ibid.
- ³⁰³ Kimberly Kitteringham and Andrew Brouwer, interview by Joshua Franklin via telephone, June 10, 2011.
- ³⁰⁴ Canada-Europe Transatlantic Dialogue, *A Comparative Assessment of Electronic Voting* (Ottawa, ON: February 2010), page 24.
- ³⁰⁵ Office of the Returning Officer (Markham), *Internet Voting Procedures* (Markham, ON: July 22, 2010), page 5-6.
- ³⁰⁶ Kimberly Kitteringham and Andrew Brouwer, interview by Joshua Franklin via telephone, June 10, 2011.
- ³⁰⁷ Ibid.
- ³⁰⁸ Office of the Returning Officer, Town of Markham, *Internet Voting Procedures* (Markham, ON: July 22, 2010), page 7.
- ³⁰⁹ The Corporation of the Town of Markham, *Request for Proposal 339-R-09: Vote Tabulation Systems and Integrated Voting Platform*.
- ³¹⁰ Ibid., pages 17-30.
- ³¹¹ Office of the Returning Officer, Town of Markham, *Internet Voting Procedures* (Markham, ON: July 22, 2010), page 9.
- ³¹² Henry Kim, *Risk Analysis of Traditional, Internet, and other Types of Voting Alternatives for Town of Markham* (Markham, ON: June 23, 2005), page 2.
- ³¹³ Ibid., page 5.
- ³¹⁴ Ibid.
- ³¹⁵ Sean Dean, interview by Joshua Franklin via email, August 10, 2011.

Endnotes

- ³¹⁶ Canada-Europe Transatlantic Dialogue, *A Comparative Assessment of Electronic Voting* (Ottawa, ON: February 2010), page 26.
- ³¹⁷ Dean, interview by Joshua Franklin via email, August 10, 2011.
- ³¹⁸ John McKinstry, "Peterborough's experience with Internet voting" (Lecture, Policy Workshop, "Internet Voting: What can Canada Learn?," Carleton University, January 26, 2010).
- ³¹⁹ *Ibid.*, page 6.
- ³²⁰ *Ibid.*
- ³²¹ Australian Electoral Commission, *Report into Remote Electronic Voting at the 2007 Federal Election for Overseas Australian Defence Force Personnel* (Parkes ACT, Australia: April 18, 2010) page 5.
- ³²² *Ibid.*, page 4.
- ³²³ *Ibid.*
- ³²⁴ *Ibid.*
- ³²⁵ *Ibid.*
- ³²⁶ *Ibid.*, page 5.
- ³²⁷ *Ibid.*, page 5.
- ³²⁸ *Ibid.*
- ³²⁹ *Ibid.*, pages 16-17.
- ³³⁰ *Ibid.*, page 17.
- ³³¹ *Ibid.*, page 18.
- ³³² Craig Burton, interview with Jessica Myers, via email, July 31, 2011.
- ³³³ *Ibid.*
- ³³⁴ *Ibid.*
- ³³⁵ Australian Electoral Commission, *Report into Remote Electronic Voting at the 2007 Federal Election for Overseas Australian Defence Force Personnel* (Parkes ACT, Australia: April 18, 2010), page 20.
- ³³⁶ Craig Burton, interview with Jessica Myers, via email, July 31, 2011.
- ³³⁷ Australian Electoral Commission, *Report into Remote Electronic Voting at the 2007 Federal Election for Overseas Australian Defence Force Personnel* (Parkes ACT, Australia: April 18, 2010), page 8.
- ³³⁸ *Ibid.*, page 11.
- ³³⁹ *Ibid.*, page 38.
- ³⁴⁰ *Ibid.*, pages 38-39.
- ³⁴¹ Ian Brightwell, interview by Jessica Myers via email, June 15, 2011.
- ³⁴² New South Wales Electoral Commission., "iVote Background," NSW Electoral Commission website, <http://www.elections.nsw.gov.au/voting/ivote/background> (accessed May 19, 2011).
- ³⁴³ Corwin Smith, "NSW Tender for Electronic Voting System," *Articlesbase*, June 23, 2010, <http://www.articlesbase.com/print/2712519> (accessed May 19, 2011).
- ³⁴⁴ New South Wales Electoral Commission., "iVote Background," NSWEC website, <http://www.elections.nsw.gov.au/voting/ivote/background> (accessed May 19, 2011).
- ³⁴⁵ New South Wales Electoral Commission, "iVote Overview," NSWEC website, <http://www.elections.nsw.gov.au/voting/ivote/overview> (accessed May 19, 2011).
- ³⁴⁶ Ian Brightwell, interview by Jessica Myers via email, June 15, 2011.
- ³⁴⁷ *Ibid.*
- ³⁴⁸ *Ibid.*
- ³⁴⁹ New South Wales Electoral Commission, "iVote Overview," NSWEC website, <http://www.elections.nsw.gov.au/voting/ivote/overview> (accessed May 19, 2011).

Endnotes

- 350 Ibid.
- 351 Ibid.
- 352 Ibid.
- 353 Ibid.
- 354 Ibid.
- 355 Ibid.
- 356 Ibid.
- 357 Ian Brightwell, interview by Jessica Myers via email, June 15, 2011.
- 358 New South Wales Electoral Commission, *Technology Assisted Voting Audit: Pre-Implementation Report* (Sydney, Australia: March 7, 2011), page 4.
- 359 Ibid.
- 360 Ibid., page 4-5.
- 361 Ibid., pages 11-13.
- 362 New South Wales Electoral Commission., "iVote Background," NSWEC website, <http://www.elections.nsw.gov.au/voting/ivote/background> (accessed May 19, 2011).
- 363 Ibid.
- 364 New South Wales Electoral Commission, *Report on the Feasibility of providing "iVote" Remote Electronic Voting System* (Sydney, Australia: July 23, 2010).
- 365 Ibid., page 56.
- 366 Ibid., pages 57-58.
- 367 New South Wales Electoral Commission, "iVote Overview," NSWEC website, <http://www.elections.nsw.gov.au/voting/ivote/overview> (accessed May 19, 2011).
- 368 New South Wales Electoral Commission, *Report on the Feasibility of providing "iVote" Remote Electronic Voting System* (Sydney, Australia: July 23, 2010), page 25.
- 369 Ibid., page 27.
- 370 Ibid., page 56.
- 371 New South Wale Electoral Commission, "Risk Management Policy," NSWEC website, http://www.elections.nsw.gov.au/_data/assets/pdf_file/0004/80869/NSWEC_Risk_Management_Policy_Vs010710.pdf (accessed May 19, 2011), page 1.
- 372 New South Wales Electoral Commission, *Report on the Feasibility of providing "iVote" Remote Electronic Voting System* (Sydney, Australia: July 23, 2010), page ii.
- 373 Craig Burton, interview with Jessica Myers, via email, July 31, 2011.
- 374 Ibid.
- 375 Victorian Electoral Commission, *The 2010 Victorian State Election Deployment of Electronically Assisted Voting (EAV)* (Victoria, Australia: July 2011), page 4.
- 376 Ibid., page 12.
- 377 Ibid., page 14.
- 378 Craig Burton, interview with Jessica Myers, via email, July 31, 2011.
- 379 Victorian Electoral Commission, *The 2010 Victorian State Election Deployment of Electronically Assisted Voting (EAV)* (Victoria, Australia: July 2011), pages 14-15.
- 380 Ibid., page 21.
- 381 Ibid., page 33.
- 382 Ibid.
- 383 Ibid.

Endnotes

³⁸⁴ Ibid., page 4.

³⁸⁵ Craig Burton, interview with Jessica Myers, via email, July 31, 2011.

³⁸⁶ Ibid.

³⁸⁷ Victorian Electoral Commission, *The 2010 Victorian State Election Deployment of Electronically Assisted Voting (EAV)* (Victoria, Australia: July 2011), page 4.

³⁸⁸ Ibid., page 33.

³⁸⁹ Ibid., page 13.

³⁹⁰ Ibid., page 62.

³⁹¹ Ibid., pages 49-51.

³⁹² Ibid., page 25.

³⁹³ Ibid.

³⁹⁴ Ibid.

³⁹⁵ Ibid., page 26.

³⁹⁶ Ibid., page 27.

³⁹⁷ Ibid., pages 28-29.

³⁹⁸ Ibid., page 108.

³⁹⁹ Ibid., page 109.

⁴⁰⁰ Ibid.

⁴⁰¹ Ibid., page 108.

⁴⁰² Ibid., page 109

⁴⁰³ The Electoral Commission, *Electronic Voting: May 2007 Electoral Pilot Schemes* (London, UK: May 2007), page 2.

⁴⁰⁴ National Institute of Standards and Technology, *Security Considerations for Remote Electronic UOCAVA Voting* (Gaithersburg, Maryland: February, 2011).

⁴⁰⁵ U.S. Election Assistance Commission, *UOCAVA Pilot Program Testing Requirements* (Washington, D.C.: March 24, 2010).

⁴⁰⁶ National Institute of Standards and Technology, *A Threat Analysis on UOCAVA Voting Systems* (Gaithersburg, Maryland: December 2008).

⁴⁰⁷ U.S. Election Assistance Commission, *Uniformed and Overseas Citizens Absentee Voting Act Registration and Voting Processes* (Washington D.C.: April 6, 2011).