e-Voting Security Study

Issue 1.2

31 July 2002

Table of Contents

1. Introduction

1.1 Background

1. Recent elections, both local and general, have seen a gradual decline in overall percentage of the electorate exercising their right to vote. This is worrying from a democratic point of view in that, if the decline is unchecked, the mandate of those elected to govern might eventually be undermined. Arguably, too, the result of an election might be more susceptible to a concerted attack of mass fraud when there is a low turnout. The government has proposed [1] a number of possible methods for re-engaging the electorate in the democratic process. One of them is to modernise the way in which the UK conducts elections. Recent changes enabled by the Representation of the People Act 2000 include: universal postal voting, an extension of the polling hours and more modern methods of casting votes, including the use of telephone and Internet based voting.

2. The government has also signalled its desire to be able to use electronic voting at general election level by the next election after 2006; and the Spending Review has allocated substantial funds to pilots at local government level in the next three years

3. A separate study was commissioned from a team led by De Montfort University [2] on the need for democratic renewal and the modernisation of electoral processes; this includes the consideration of perceived barriers to implementing electronic voting. Its report was published on 23 May 2002.

4. It was in this context that CESG, the UK's National Technical Authority for Information Assurance, was invited by the Office of the e-Envoy to study the risks of new electronic methods, and to develop a set of security requirements by which any future implementation could be measured. Predominantly these fall into two broad categories:

   - enabling the ballot to be conducted in a manner where votes are secret;
   - providing a reliable and secure infrastructure, over which the votes are transported, collected, counted and audited.

5. The Department for Transport, Local Government and the Regions (DTLR) ran a number of trials using different voting methods in the local elections held in May 2002. However, it is not the purpose of this study to provide any security analysis of these pilots. The independent Electoral Commission has conducted a separate evaluation of the pilots, as required by statute.

1.2 Aims & Objectives

6. The defined aims and objectives of the study were as follows:

   - to outline plausible approaches to electronic voting in UK elections, covering options for methodology, infrastructure and voter experience;
   - to assess the security risks associated with each;
   - to postulate mechanisms for mitigating those risks to the point where the Government might be expected to consider them acceptable in a UK general election;

- to assess the potential for (and benefits and disadvantages of) applying those mechanisms to multiple electronic channels (and, if appropriate, non-electronic channels as well);
- to report accordingly, with recommendations, to the Study Steering Group.

7. The study was also expected to inform concurrent work by the OASIS group in respect of XML standards for e-voting systems.

1.3 Report Structure

8. This report has the following structure:

- Delivery Channel Analysis – provides a security review of the proposed delivery channels for e-voting;
- Prior Art Review – summarises the academic and commercial setting for work already conducted in this area;
- Conclusions and Recommendations;
- Annexes;
    - General e-voting Security Requirements
    - Summary of Background Review
    - Possible technique based on scratch cards

1.4 Definitions

9. 'E-voting' is a current 'buzz word'; and encompasses all voting techniques involving electronic voting equipment; however for the purpose of this report e-voting is too broad a term and the following more specific definitions will be used.

- **electronic voting (or e-voting)**: any voting method where the voter's intention is expressed or collected by electronic means.
- **electronic counting**: specifically used to cover technologies that electronically count physical ballots, such as optical scanning of ballot papers.
- **kiosk voting**: in the electronic context, kiosk voting means the use of dedicated voting machines in polling stations or other controlled locations. Voters mark their choice electronically (perhaps on a touch sensitive screen) rather than on a paper ballot. The votes are counted on individual machines, known as Direct Recording Electronic (DRE) machines, and the votes cast are transferred to the central tallying point by unspecified means. A ballot paper can be printed and retained in confidence in a ballot box as an additional check.
- **remote electronic voting (REV)**: this is the preferred term for voting that takes place by electronic means from any location. This could include the use of the Internet, text message, interactive digital TV, or touch-tone telephone.
- **online voting**: taken literally this means voting in an electronic way while connected to a live system. It therefore includes not just REV, but also forms of kiosk voting where there is a permanent connection to a central server.
- **Internet voting (or i-voting)**: a specific case of remote electronic voting whereby the vote takes place over the Internet such as via a web site or

voting applet. Also sometimes used synonymously with Remote Electronic Voting. That usage is however deprecated and it will instead be used as a strict subset of REV.

- **online election system**: the physical system responsible for handling the online election process.
- **client**: the device which the voter uses to interface with an online election system
- **voting server**: a generic term for server components of an online election system.
- **personation**: the act of fraudulently voting in someone else's name.

2. Initial Analysis of Delivering E-voting

10. The following diagram illustrates how e-voting may work in practice. Voters would send their e-votes through their client device of preference. These devices would normally be connected to a public network (i.e. the Internet or the PSTN), via a service provider. The vote would then be routed from the service provider to a vote collection and processing centre, via a public or private network.

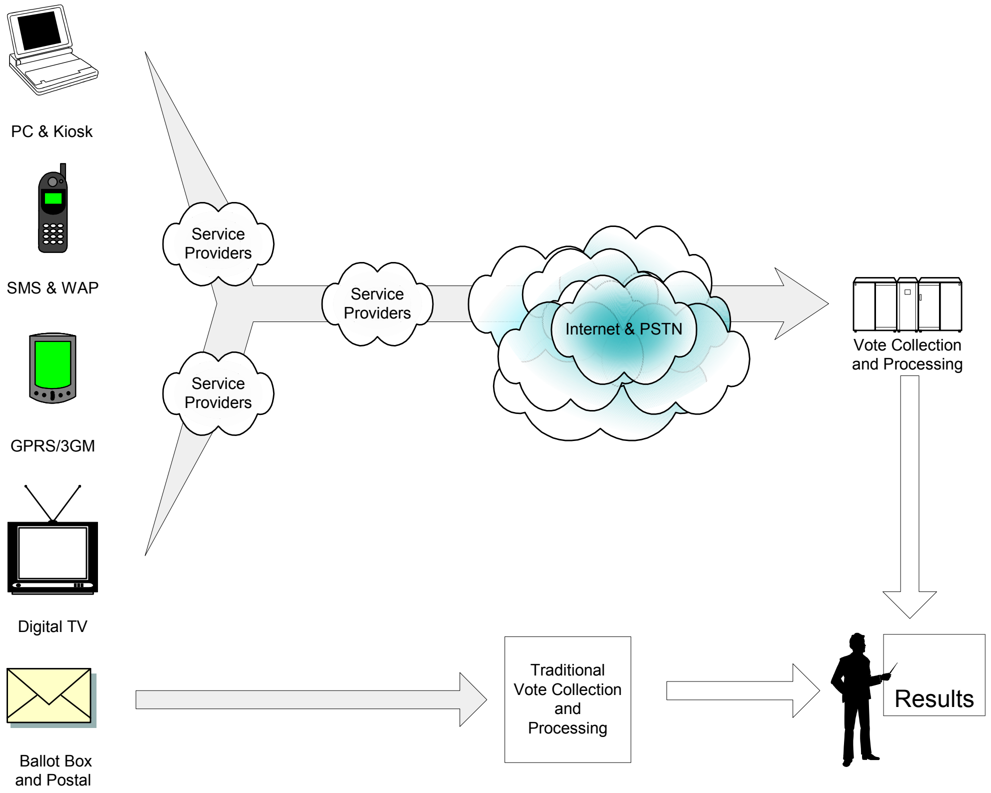

Figure 1: E-voting Delivery Architecture

11. The challenge these devices pose vary considerably, from the very limited interface of the telephone to the very rich and complex Personal Computer. The following sections outline a few of the challenges – some relating to security, some usability – which these devices pose.

2.1 Telephone

2.1.1 Touch-Tone Telephone

12. Any modern phone on a digital exchange that uses tone instead of pulse dialling can be used for remote electronic voting. Although many touch-tone telephones have letters written above the numbers, the number-based dial tones available at the handset limits the richness of the interface.

13. Whilst the fixed-line Public Switched Telephone Network offers significant confidentiality and integrity, it does not offer services which identify the individual who is making a call, though it could possibly identify which telephone line was use to make the call.

14. Touch-Tone Telephony is therefore best suited to voting applications based purely on numeric data e.g. where the voter receives unique numeric security

data (e.g. voter number, PIN) and a personalized number for each candidate. Responses can be spoken by an automated voice. No special purpose client processing is available.

2.1.2 Voice-Activated Telephone

15. Voice-activated calls are similar to touch-tone calls, although the richness of the interface is limited by the ability of generic voice processing software to identify basic words such as “yes, no, one, two or three”.

16. Voice-Activated Telephony is therefore not recommended as a user interface. It has many potential weaknesses, and Touch-Tone Telephony is better than Voice-Activated in every respect, apart from the fact that a small number of households are still not served by digital telephone exchanges.

2.1.3 SMS (Text Messaging)

17. The vast majority of mobile telephones currently in use are enabled for text messaging, also known as Short Messaging Service (SMS.). SMS messages can contain upper- and lower-case letters, numbers, and punctuation/symbols. Intercepting SMS amounts to the same problem as intercepting mobile telephone calls.

18. Although there are Internet services that allow text messages to be sent, many of these do not give the sender any opportunity to receive a text-message in return, and consequently would be unsuitable for REV applications that require a response to be sent to the voter.

19. As SMS is inherently a "best effort" delivery medium with no guarantee of successful delivery, this effectively rules out such Internet-based gateways, as a response will be required to satisfy the voter that their vote has been received. In fact, this response may have to be sent multiple times to increase the likelihood of at least one getting through.

20. SMS is suited to voting applications where the voter receives unique alphanumeric security data (e.g. voter number, PIN) and a personalized numbers for each candidate. Responses would take the form of SMS messages, and may have to be sent several times. It is unlikely that attempts at multiple voting could be penalized, as some voters may legitimately send their vote twice if they do not receive a response to the first attempt. Again, no client processing can be used, as there is no client.

2.2 Interactive Digital Television

21. IDTV takes one of two forms: cable and non-cable. Non-cable IDTV (terrestrial, satellite) is made interactive by use of a telephone line. Cable TV communicates over the cable company's cable infrastructure.

22. It may be possible to modify set-top box software to add an electronic voting application to facilitate client processing. Whether this can be done and rolled-out securely enough would be a matter for investigation, and whether it would be feasible to create enough versions to run on every possible type of set-top box, on-time, and for a reasonable budget, is also doubtful.

23. Most set-top boxes do, however, offer a user interface that allows the selection of options and input of alphanumeric data. Although this lacks client-processing power, this makes for a system with a fairly reliable transport for responses that has similar risks to using touch-tone telephones, and a richer user interface.

2.3 Internet

24. The richness of the Internet allows a number of ways to enable remote electronic voting. The capabilities of these systems will depend on the client assumptions you are willing to make. A range of alternatives is presented below.

2.3.1 Simple Web Form

25. A simple web form would be a web page that allows alphanumeric data to be input and a response to be returned, rather like the SMS and IDTV methods outlined above.

26. Any data that traverses the Internet is potentially at risk of modification by the intermediate computers and networks that it passes as it traverses from endpoint to endpoint. The route is not well-defined and is susceptible to malicious modification.

27. As a simple web form does not assume any end-to-end encryption or authentication, there is a reliance on the security-critical data being communicated to the user in advance, such as voter number and PIN, as well as personalized candidate codes. In many ways a simple web form is like IDTV, albeit more widely accessible.

2.3.2 SSL Website

28. A Secure Sockets Layer (SSL) protected website would be similar to a shopping experience – the user enters authentication data and then picks the candidate that for which she wishes to vote from a list.

29. This would be easy to use, but is not without risks above those incurred in distributing user names and passwords.

30. This method also relies on the browser and operating system of the user processing the user's intention into a vote for the correct candidate, and sending it down the wire.

31. It would be perfectly possible for a virus to modify the client web browser or operating system so that when a user clicks or presses a key to vote for a particular candidate, a different intention is passed to the server. Such a virus could be distributed as a worm, or trojan (like *ILoveYou* , *Nimda, or CodeRed*), and rely on known, but unpatched, vulnerabilities in operating systems.

2.3.3 Mobile Code (Java Applet)

32. A user could authenticate to an SSL website and then download a Java applet that runs within the web browser and enables local client processing, for example to digitally sign a vote. This digital signature could use an existing public key infrastructure, or one created especially for the voting. The authentication would have to be anonymous.

33. It is worth noting that many of the academic assessments of remote electronic voting assume some intelligence in the client and therefore condemn the concept owing to weaknesses in the client, whereas they are in reality condemning our inability to gain enough trust in client operating systems and software.

2.4 Voting Operating System

34. Proposals exist for creating specific operating systems for voting. This operating system could then be distributed to voters on CD-ROM, and voters would boot off that CD-ROM, configure their Internet or modem connection, and then vote.

35. This would allow a greater degree of trust to be had in the operating system. However it is costly and complex to create and distribute the operating system, and probably costlier still to support and maintain it. There may also be legal issues, such as liability.

36. Also, it is very unlikely that all PC hardware platforms could be supported with one custom operating system, and the requirements placed on the user (essentially configuring Internet access) would frustrate all but the technically literate. There would also be a risk of someone creating a modified version of the trusted OS that does not act in a trustworthy way.

3. Summary of Background Review

37. The subject of electronic voting is not new. Thomas Edison received US patent number 90,646 for an electrographic vote recorder in 1869. Since then, much work has been done on remote electronic voting in both the academic community and by a number of commercial companies. A summary of the background review on work already conducted in this arena follows; the full version of the review can be found in Annex B.

3.1 Academic

38. The bulk of academic opinion is against the use remote electronic voting in major elections. Two main reasons are cited: security of the process, and the possibility of coercion. This has not stopped a steady flow of academic papers that attempt to address the associated problems.

3.1.1 Personal Views and Testimony

39. A number of well-known academics such as Prof. Ronald Rivest of MIT believe that home computers are not secure enough to facilitate electronic voting [14].

40. Many of academics have concerns about privacy. These are largely US academics and the concerns are less significant under the current UK practice of publishing the identities of those who voted, because it is hard to prevent an eavesdropper from seeing the telephone number or Internet IP address of someone who is voting.

41. The issue of coercion applies to any remote voting, whether electronic or postal. Many academics are opposed to both as they may allow verifiable vote selling - a voter's credentials can be sold to a malicious individual who can then vote for the 'correct' candidate.

42. To fully address the possibility of coercion, REV should not use credentials that can easily be sold as a whole and should not allow a voter to prove how they voted after the event (e.g. by providing a detailed receipt). No system exists which meets these requirements.

43. Academic opinion does not object in principle to kiosk machines in controlled places to record votes. Machines that both count votes and print ballot papers for deposit in ballot boxes are preferred, as they offer a paper audit trail.

3.1.2 Proposed Solutions and Protocols

44. The foundation of much of the academic work in the area is a paper by Fujioka, Okamoto and Ohta entitled "A practical secret voting scheme for large-scale elections" [4]. There have been a number of published improvements on the paper, including Dr. Lorrie Cranor's Sensus protocol [5] and even practical implementations for university-wide elections such as E-Vox, which has been used at MIT [6].

45. Academic protocols frequently gloss over client issues and instead focus on the back-end security of the system. This is an important area for large-scale electronic voting as it is desirable to minimise the potential damage that can be caused by a single failure or malicious act.

46. The essence of Fujioka *et al*–style protocols is to separate the back-end functionality of a system so that separate functions are provided by subsystems such as distribution of ballots, authorization of voters, collection/storage of

ballots, decryption of ballots, and the counting of votes. Subsystems can be isolated and the flow of data between them can be minimised.

47. For example, one technique proposed to separate authorization from collection is a blind signature. Blindly signing a document is signing a document without knowing what its contents are. So a voter presents an encrypted ballot to the authorizing system, and the encrypted ballot is signed and returned to the voter if the voter is eligible to vote.

48. With the right choice of encryption and signature scheme - technically, if the blinding encryption and signature commute - the voter can strip off the blinding encryption and then is free to anonymously and securely submit the signed ballot to the collection system. Because the ballot has been signed it is counted as a valid vote. The authorizer and collector never need communicate.

49. A crude physical analogy to blind signatures is handing ballot papers to people as they walk into a polling station. People then fill out their ballot papers and present them upside down ("encrypted") to the election official. At this point the election official ticks the voter's name off and embosses the ballot (the blind signature). The ballot can then be placed in the ballot box, and only embossed ballots get counted.

3.2 Commercial

50. Commercial implementations of electronic voting aimed at large elections can be divided into three main technology types:

51. The simplest merely requires that voters are sent user IDs and PINs in the post. Voters then vote by sending their user ID, PIN, and a number representing their chosen candidate. This technology was used by election.com in the 2002 local election trials in Sheffield and Liverpool.

52. Slightly more complex is to use a password-protected website. Voters are sent authentication information that they use to log in. They can then click next to their candidate of choice and submit a vote. This type of technology was used in a couple of the 2002 local election trials.

53. More complex systems on the market require client code, typically a Java applet within a web browser. Such solutions provide a richer client and richer user interface. They also add many risks and are yet to be seen in large trials.

3.3 Other National Voting Pilots

54. There are a number of studies in place in various national and international bodies that are investigating electronic voting. There have also been trials outside of the UK. Some highlights are given below.

3.3.1 Europe

55. The three-year EU Cybervote Project ends in March 2003 and has so far produced a number of technical reports on Internet voting technologies. Their website is at www.eucybervote.org.

56. Trials exist, for example in the Netherlands, for kiosk voting that will not tie an individual to a particular polling station. This will allow voters to cast their ballot from any convenient polling station.

3.3.2 US Pilots

57. For the November 2000 US Presidential Elections, a small number of Department of Defense employees who were posted away from home were allowed to cast their absentee ballots via the Internet.

58. This worked well for a small number of trusted users who were enrolled in the DoD Public Key Infrastructure. The system had particular software requirements, but the fact that everyone had access to DoD computers made this less of an issue. The upshot of the pilot was that the Internet voting worked well for a small number of DoD employees, but this system would require a national PKI to scale.

4. Conclusions and Recommendations

4.1 Overview

59. In determining our recommendations we concluded that the following principle would be key in the development of any successful, and secure, Remote Electronic Voting system. This principle outlines the requirement for a trusted path between the voters' intention and what is recorded by the system. This, in a traditional system, is the essence of pencil, paper and ballot box.

Key Principle

The signalling of intent, by the voter, into the electronic environment should have no observable properties, and the voter should receive assurance that their vote was recorded as it was intended.

60. Whilst conducting this study we concluded that the current UK voting system is not perfect. For instance it is possible to turn up at a polling station and claim to be anyone on the electoral register, within that particular ward, and you should be given a ballot paper.

61. However, it is probably impossible to make any system perfect. This leads to the conclusion that a sensible risk management-based approach needs to be established, and specifically the level of risk that is acceptable to the UK electoral system must be determined. In financial systems either an insurance policy or higher prices underwrite the level of risk. In an e-democracy system what would be an acceptable level of misuse?

62. In developing this study we have seen that there are possible abuses of the current system, and any electronic system must be shown to be at least equally secure. However, mass fraud in the current system is particularly difficult to arrange. Given the nature of e-voting systems it is likely that, rather than calling a single constituency result into question, the whole election result may fall into doubt. Steps must be taken to ensure that this worst-case scenario does not occur.

63. To this aim we have developed a statement of general security requirements that should be applied to all new pilots and any future national e-voting implementations.

Recommendation 1

The security profile in Annex A to this study should be used as a basis for discussion in the development of any future pilots and full-scale e-voting implementations.

4.2 Threat

64. After consultation with the UK's threat authorities, it is clear that e-voting in a General Election would be a significant and attractive target. These 'hacktivists' are currently considered the most likely source of threat to a General Election, however as world events change it is possible that better resourced and technically capable threats will emerge.

4.3 Client Devices

65. There is a vast range of client systems, and their capability varies greatly from those that have very restricted environments to those that are immensely powerful and flexible. Current academic protocols designed to resolve some of the problems surrounding e-voting require the client platform itself to have some computational power. This assumption would severely limit the channel that can be used, probably to Internet-connected computers.

Recommendation 2

E-voting systems should use techniques that do not require specialised applications at the client in order to secure the system.

66. Usability concerns also need to be considered. Having a different set of credentials for each possible client/delivery channel access will be potentially confusing for any voter. Any system used for e-voting should be designed to keep the overhead of multiple sets of credentials to a minimum.

Recommendation 3

E-voting systems should use techniques that are consistently supported across a broad range of client devices.

4.4 Delivery Mechanisms

67. Mechanisms for votes to be cast need to have three properties: confidentiality, integrity and availability. A delivery mechanism is the combination of a voting protocol and a delivery channel. The use of secret information passed to the voter out-of-band is likely to reduce the requirement for the delivery channel service provider to support a specific e-voting confidentiality and integrity service.

Recommendation 4

An appropriate mechanism should be chosen to negate the requirement for the delivery channel infrastructure to provide confidentiality and the integrity of the vote.

68. Availability will be harder to address. Attacks on the availability of a channel can be both electronic and physical. Primarily the infrastructure networks of concern will be the fixed line PSTN, mobile telephone networks and the Internet.

Recommendation 5

Measures need to be taken with both the infrastructure providers and any e-voting service providers to ensure an acceptable level acceptable of availability of e-voting systems.

4.5 Security Techniques

69. While recommending that e-voting systems should employ security mechanisms with the properties addressed in our previous recommendations, we do not believe that current security technologies are able to meet all these requirements. We have considered the use of scratch-card like solutions in

Annex C and believe they currently offer the best approach to meeting the requirements. The mechanisms detailed in Annex C are only an exemplar of how a ‘first past the post’ secure electronic ballot could be achieved and should not be considered a final solution. They are, as yet, untested on a large scale.

Recommendation 6

A set of security concepts and mechanisms, similar to those proposed in Annex C, should be piloted in the next set of local elections.

Recommendation 7

The government should consider how to extend the concepts and mechanisms proposed in Annex C to electoral systems other than ‘first past the post’.

70. The use of such techniques changes the voting paradigm significantly; from being able to vote by demonstrating the right to vote, to, being able to vote only through the possession of a voting token. They also bring in wider security concerns associated with the distribution of the tokens to the electorate through the postal service.

Recommendation 8

The Electoral Commission should study the implications of the significant change in the voting paradigm which would arise from the use of different security techniques.

4.6 Assurance & Accreditation

71. There are a number of methodologies that can be used to provide assurance in the security of any voting system. How these methodologies can be combined and used depends very much on the architecture of the final solution. These range from very formalised solutions such as the Common Criteria Certification to ad hoc solutions such as independent examination and inspection, a more complete list is provided in Annex A.

Recommendation 9

A study on the assurance requirements for any e-voting service should be conducted.

72. HMG has developed a methodology for providing the accreditation of government computer systems. The government needs to determine the most appropriate method of accrediting any national voting system(s).

Recommendation 10

The accreditation requirements for national voting solutions should be determined.

4.7 Multiple Voting

73. Enabling the use of multiple voting channels opens up the possibility of a voter casting their vote across a number of different channels, or many times across the same channel; these votes may all be for the same or for different candidates.

74. This creates the problem of determining which vote should count. There are a number of possibilities:

- precedence is based on the channel that delivered the vote
- precedence is based on the time the vote was sent, in this case you could select:
    - the first vote received; or
    - the last vote received

75. In addition, if postal and traditional balloting are to continue as voting channels there will be added complexity in delivering the final result. If traditional ballot or postal balloting did not take precedence, each paper ballot associated with a voter who had voted electronically would have to be removed from the count by hand. This will be time consuming.

Recommendation 11

The Government should consider with the Electoral Commission the rules to govern precedence where multiple voting is used.

76. Although it is sometimes claimed otherwise, multiple voting cannot always provide a solution to coercion. With a system where the last vote counts it would indeed possible for a voter to change their mind if previously coerced. However if the voting relied on physical credentials that can be stolen then the coerced voter could not change their mind. Similarly, if the last vote were counted then voters will have to keep their credentials secure until the close of poll, and would be open to coercion until the end of the poll. Additional threats would also be introduced to some voting protocols.

Recommendation 12

The Government should ensure that the issues associated with coercion and multiple voting are studied.

4.8 Vote Confirmation

77. A number of the electronic delivery channels cannot be considered ‘reliable’ in terms of guaranteeing the delivery of the vote (e.g. SMS). In these instances, CESG would normally advise that an acknowledgement message be sent back to the voter in order to provide reassurance that their intended vote had been cast, as without such a message the voter is unsure whether their vote has reached their intended target or has been intercepted and changed.

78. However, vote acknowledgement would open up the possibility of verifiable vote selling, where organisations might pay individuals for voting, and proving that they had voted, in a particular manner.

Recommendation 13

The government should ensure that the use of vote acknowledgements and the risks of vote selling/vote fraud are studied.

4.9 Future Pilots

79. In assessing the possibilities of secure electronic voting we have discussed the types of architectures that would be used to deliver such a system. Work currently being performed by the OASIS EML group appears to be promising and we would encourage the development of the OASIS protocols in future trials.

Recommendation 14

Any future trials should assess how e-voting services can be delivered on a larger scale and, should include the ability to regionalise services.

4.10 Independent Scrutiny

80. Whilst we believe our proposals and recommendations make secure e-voting possible, we have reported more pessimistic academic opinion. Ultimately the electorate will only have trust and confidence in any new electoral process if a substantial body of informed opinion supports our proposals.

Recommendation 15

The government should consult the public, academic community, and commercial suppliers to establish whether these proposals can command broad support.

Annex A. Preliminary Statement of Security Requirements

A.1 Introduction

81. This annex provides a preliminary statement of security requirements for Remote Electronic Voting systems. This section of the study has been developed so that it is consistent with the primary work on e-Government Security [3].

A.1.1 Security Requirements Approach

82. The vehicle for requirements expression is based upon the Protection Profile concept developed for the international security evaluation criteria (Common Criteria).

83. The requirements expressed in this study represent a baseline for discussions as to what constitute adequate and acceptable security measures for e-voting. It is recognised that, subject to a risk assessment, not all the requirements may be applicable in all cases, and that in some cases it may be technically or economically infeasible to meet the requirements fully.

A.2 Security Environment

A.2.1 Environmental Assumptions

84. It is assumed that the delivery of e-Voting services will take place across networks that are commonly available to the electorate. These are likely to be the PSTN, the mobile phone networks, the Internet and digital TV channels. The security domain model is illustrated in figure 2.

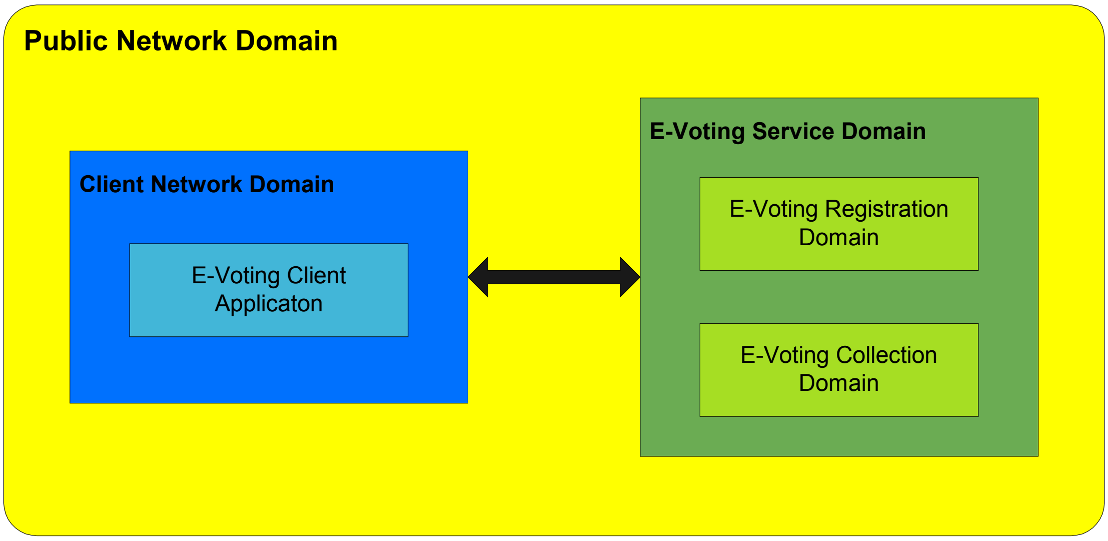
Public Network Domain
E-Voting Service Domain
Client Network Domain
E-Voting Registration Domain
E-Voting Client Applicaton
E-Voting Collection Domain

Figure 2: Security Domains

85. The **Public Network Domain (PND)** contains that part of the communications infrastructure not under the control of the e-Voting Service operators and clients. In the case of Internet delivery, it must be assumed to be accessible to potential threat agents and to provide a transmission capability with no service quality elements (e.g. integrity or confidentiality). In the e-voting context, the PND

includes the Internet, the PSTN, mobile phone networks and interactive digital TV channels.

86. The **e-Voting Service Domain (EVSD)** contains that part of the communications infrastructure that is under the Returning Officer's control and is used to host the e-voting registration and collection services.

87. The **e-Voting Registration Domain (EVRD)** contains IT infrastructure to host all or part of the electoral registration process. The EVRD may extend to facilities beyond the authorities immediate control for processes such as secure printing to facilitate the authentication of e-voters.

88. The **e-Voting Collection Domain (EVCD)** contains the IT infrastructure to host all or part of the ballot collection process. The EVCD should be physically separate from the EVRD to facilitate the anonymisation of ballots.

89. The **Client Network Domain (CND)** is that element of the infrastructure under the control of the client, which is used to support access to the e-voting service. It is likely that the CND will be a single domestic personal Computer connected via an ISP to the EVSD, in this case the ISP lies within the PND or it could be a WAP enabled mobile phone where the service provider's WAP gateway lies within the PND.

90. The **e-Voting Client Application (EVCA)** is that element of the CND that is supplied by the e-Voting service and is installed within the CND to encapsulate important trusted elements of service. The e-voting service management will exercise some control over the content (but not necessarily the delivery of) the EVCA.

A.2.2 Legislative Requirements

91. The following are the principal pieces of legislation and proposed bills that inform e-voting implementations:

- the **Computer Misuse Act** makes attempted or actual penetration or subversion of computer systems a criminal act;
- the **Data Protection Act** set requirements for the proper handling and protection of personal data held in information processing systems;
- the **Representation of the Peoples Act(s)** set requirements for voting security and scrutiny.

A.3 Threats to e-Voting Services

92. Remote Electronic Voting (REV) breaks down the geographic barriers of traditional election systems. The election system is no longer confined to the local polling station; it is accessible world-wide, increasing the potential number of attacks dramatically.

93. By its very nature, the election process is an attractive target for malicious actions. An online voting system would need to win public confidence, which could easily be undermined by an election-day horror story.

94. No assumptions are made in what follows with regards to the configuration the REV system. The assessment is based on the assumption that the REV system will have external connections, affording external access, and the information will potentially be available online and of a personal nature (i.e. subject to the Data Protection Act).

A.3.1 Potential Sources of attack

A.3.1.1 Internal

- Legitimate users

  Legitimate users of the REV system may seek to misuse or damage the election system and may have significant technical resources and skills at their disposal, with a strong motivation to subvert the service - frequently for financial gain. Since they are legitimate users, they are subject to legal sanctions if the subversive activity is traced to them.

- REV System operators

  The REV System operators may seek to exploit their privileged position. They may include government employees or their agents or employees of outside organisations contributing to REV services. Such individuals may possess significant resources and technical skills in addition to privileged access rights. Their motivation could be desire to defraud the election process, either for financial gain or personal satisfaction. Service operators and government employees are readily subject to sanction in the event that security breaches are traced to them.

- Other Insiders

  Government employees and their agents who may have access to the REV system, but are not associated with the provision of election services, may conduct insider attacks. These individuals may possess a strong motivation to mount an attack for financial or personal gains. Such individuals will be readily subject to sanction.

A.3.1.2 External

- Hostile Individuals

  Individual hackers may seek to cause disruption to systems because of a personal grudge, for the challenge of attacking a government system or in protest against government policies. They may also wish to access, corrupt or steal data, either for personal gain or for publicity purposes.

- Criminal Organisations

  Criminals or others, such as information brokers, may also wish to access systems in order to obtain personal details for exploitation.

- Protest Groups

  Protest groups or ‘hacktivists’ may seek to attack systems in order to demonstrate opposition to REV, to disrupt the e-voting mechanism or to obtain data to exploit, for information or corruption purposes.

- Foreign Intelligence Services

  Foreign Intelligence Services may see an advantage in obtaining personal information, for intelligence-gathering and targeting purposes. They may also wish to access systems for political information-gathering purposes or to manipulate voting information in order to influence the outcome.

- Investigative Journalists

  Investigative Journalists may be interested in deliberately subverting the election system in order to prove that a REV system has security flaws.

- Terrorist Organisations

Terrorist organisations may be interested in personal information stored on the system for targeting and intelligence-gathering purposes. They may also wish to interrogate the system in order to understand voting intentions, to affect the outcome or to cause disruption to the process.

A.3.2 Possible Methods of attack

A.3.2.1 Electronic Attack

- Hacking

  Penetration of the REV System would have very serious ramifications, both for public confidence in online voting and with regards to statutes such as the Data Protection Act. To be effective, such an attack need not even modify the data stored in the system, merely put it into the public domain. Penetration of the system need not take place during the polling period, but potentially any time after the event. Large amounts of personal information used by the voters to authenticate themselves in the registration phase may be divulged. This information could be used to link votes with individuals, undermining voter anonymity. There is also the potentially less serious threat of the appearance of the site being changed; this would undermine public confidence in the system. If the hyperlinks on the site were changed this could affect the integrity and confidentiality of the votes cast; this might result in the election being declared void.

  Individual client platforms are unlikely to be attractive targets for the hacker. However public Internet terminals would provide an attractive target and would need to be secured accordingly.

- Malicious Software ('malware')

  There is a risk of introduction of malicious software being introduced onto the REV server before or during the election, via email or an external communications link. Furthermore, the connection of huge numbers of PCs to the REV system may increase the chances of malware being spread to the REV Server. This could cause damage to the server and potentially propagate to other PCs. The government could potentially be liable for any resultant damage. If a program such as a 'Trojan Horse' were to be installed on the REV server, the confidentiality and integrity of the votes could be adversely affected, in the worst case resulting in an election being declared void.

  The insecurity of browsers and operating systems on the client platform will invariably make it possible to subversively install malicious software. It is possible for an attacker to introduce malware that has an activation delay on to the client platform, where it would remain undetected until activated on the date of the election. Installation of a program such as a 'Trojan Horse' could compromise the confidentiality and integrity of an individual's vote, by communicating information on how an individual voted to a third party, or by changing the vote before transmission without the user's knowledge respectively.

- Denial of Service

  An exceptionally high volume of voters using the REV may cause the REV to become temporarily unavailable. A malicious attack or mass unintentional misuse may also cause the REV system to become unavailable, either temporarily, or in the worst case for the duration of the election.

The client may be denied service by an attack on the delivery channel. It is also possible that a client device is attacked using a program to initiate a large number of redundant computations, which could render the device useless.

- Domain Name Service (DNS) Attacks

  It is possible that an attacker may alter an entry in a DNS lookup table to point to a bogus web address. This would enable the owner of the bogus Site to undermine the vote of the redirected voter. The same effect can be achieved by introducing a program that tells the browser to use a certain web address as a proxy, essentially affording a 'man-in-the-middle' attack.

A.3.2.2 Other attack approaches

- Vote buying/ selling and coercion

  Such activities are only possible on a small-scale as a large operation would be difficult to orchestrate without being detected.

- Theft or forgery of election details

  Theft and forgery of voter details is possible either electronically or from the postal system, if it were used. Once again this is unlikely to occur on a large scale since such activities would be detectable.

- Deliberate repudiation of transaction

  An attacker could potentially go to the media and claim "I did not vote that way!" This could be used in an attempt to undermine online voting; how credible such a claim would be is questionable.

- Accidental damage
  - Users

    Legitimate users may unintentionally misuse the REV System and potentially cause damage to the System. Large numbers of voters using the System incorrectly could result in unnecessary loss in performance of the System or even causing it to crash.

  - Operators

    Operators may, through incompetence or inadequate training, cause damage to the system or loss of data. Such individuals are not specifically motivated to carry out such an attack but, due to their privileged access rights, may unwittingly cause significant damage.

  - Equipment

    Equipment or software failure may lead to suspension of service or loss of information.

  - 'Acts of God'

    An accident or other natural disaster may destroy the service provision or stored information.

A.4 Security Objectives

A.4.1 System/Service Control Principles

95. In determining what the principal security controls for an e-voting system should be we have reviewed a number of criteria available, including those of the California Internet Voting Task Force. We have compiled a best-of-breed set of principles from those available:

- **Voter Authenticity** – ensuring that the voter must identify themselves (in some manner) to be entitled to vote;
- **Voter Anonymity** – ensuring that votes must not be associated with voter identity, unless warranted under law;
- **Data Confidentiality** – ensuring that the vote is secret;
- **Data Integrity** – ensuring that each vote is recorded as intended;
- **System Accountability** – ensuring that system operations are logged and audited;
- **System Integrity** – ensuring that the system cannot be re-configured during operation;
- **System Disclosability** – allowing the system to be open to external inspection and auditing;
- **System Availability** – ensuring that the system is protected against accidental and malicious denial of service attacks;
- **System Reliability** – developing the system in a manner that minimises accidental bugs and ensures there is no malicious code;
- **Personnel Integrity** – those developing and operating the voting system should have unquestionable records of behaviour;
- **Operator Authentication and Control** – ensuring that those operating and administering the system are authenticated and have functional access on the system strictly controlled.

A.4.2 System/Service Control Objectives

96. The security control objective statements distil the threat, assets, environmental assumptions and security principles into a set of control objectives that, if they are all met, ensure that the threats identified are properly countered in the declared environment.

97. The objectives are necessarily high level and seek to minimise the constraints on candidate implementations. Some of the objectives will be levied on the environment and trace to security requirements that the environment must be shown to meet.

Security Control Objective	Notes
OS1 – Effective Voter Registration Voting permission is only granted to those whose bona fides have been established.	A combination of procedural and technical measures to ensure that voters are properly identified before being granted permission to vote and that multiple and false identities cannot be

Security Control Objective	Notes
	registered.
OS2 – Effective Voter Authenticity E-voting services are only available to those eligible to vote.	Access to e-voting services can only be obtained on the presentation of properly constructed access credentials.
OS3 – Effective Voter Anonymity Either during the voting process or at the ballot count the real world identity of the voter cannot be established.	A combination of technical and procedural measures to ensure that votes cannot be attributed to individuals either whilst they are voting or during the ballot count. However, under warranted conditions systems should be able to determine if gerrymandering has occurred.
OS4 – Effective Vote Confidentiality E-voting services must guarantee the confidentiality of the vote until it is counted.	A combination of technical, procedural and out of band measures to ensure that votes cannot be attributed to an individual candidate during the voting process.
OS5 – Effective System Identification and Authentication Accountable e-voting service processes are only accessible to those individuals and systems that have been authorised to access such processes.	A requirement for technical measures to ensure that access, to the ESVD, can only be obtained on presentation of properly constructed access credentials.
OS6 – Effective System Registration Access permission to e-voting service processes is only granted to those who bona fides have been established.	A combination of technical and procedural measures to ensure that users, within the ESVD, are properly identified and authenticated, and can access only those parts of the system and assets necessary to perform the authorised task.
OS7 – Effective System Access Control Access granted to e-voting service application and assets is the minimum necessary for the identified user to obtain services required.	Will map on to a requirement to ensure that a user/administrator within the EVSD, once identified and authenticated, can access only those part of the system and assets necessary to perform the authorised task.
OS8 – Information Integrity Ensuring that the voter's intention is received as intended.	Information transmitted and received by the e-voting service must not be altered or otherwise subverted.
OS9 – Service Availability Continuing access to the e-voting service as and when required must be assured	Users of the e-voting service must be able to depend on the continuing availability of the service in order for them to meet their obligation to vote – subject to limits imposed by the availability of the PND.
OS10 – Information Availability Continued access to e-voting data assets	Data assets of the e-voting service are an important record and must not be lost

Security Control Objective	Notes
as and when required must be assured.	through accidental, careless or deliberate acts of e-voting service users, or administrative staff, or in the event of equipment failure.
OS11 – Service Protection The e-voting service implementation and associated assets must be protected from external interference and penetration.	The e-voting service must be adequately protected from outside attack mounted against the service application or the underlying network infrastructure.
OS12 – Operator Integrity Those operating and administering the e-voting service should be of an unquestionable record of behaviour.	THE PERSONNEL ADMINISTERING THE E-VOTING SERVICE MAY BE IN AN ENHANCED POSITION TO ATTACK THE SYSTEM.
OS13 – Open Auditing and Accounting The e-voting service must keep a proper record of significant transactions.	A general requirement for a proper record of significant events that may have to be revisited. This will include system configuration to enable external observers to determine that no collusion could have taken place.

A.4.3 External Control Objectives

98. The principal external assumptions, also known as environmentals, that relate to the provision of e-voting services are tabulated below.

External Control Objectives	Notes
Open Delivery e-voting services are delivered over public networks over which the e-voting service provider has little or no control.	The requirement is that no government special infrastructure is necessary to deliver the services. The Internet is seen as the delivery mechanism of choice, though direct dial–in over the PSTN is also a likely possibility. No statement can be made about the assurance of the client workstation.
Existing Secure Networks The systems hosting e-voting services are installed and managed in accordance with existing policy and practice for government systems connected to other networks.	A statement about the environment, which cross-references to existing codes of practice and policy on government and other service supplier networks. It is expected that any large vote collection and counting systems should conform to current government best practice.
Unassured Client Domain e-voting services must be implemented in a way that permits adequate trust relationships without requiring strong controls or constraints on the terminals used to access the services.	The equipment used by members of the public to access the service is uncontrolled and typically under non-technical management control that is unaware of the security risks. Government cannot place constraints on the state of such equipment as a condition for e-voting service access.

External Control Objectives	Notes
	Security approaches should allow for this.

A.5 Security Requirements

A.5.1 OS1 – Effective Voter Registration

1.1	Access rights to REV services shall be granted only when the REV registration service management is satisfied that the user is actually who he/she claims to be, is not already registered under a different identity, and has a legitimate right to vote as defined by law.	An effective registration authentication mechanism to record those who claim voting rights must be in place.

A.5.2 OS2 – Effective Voter Authenticity

2.1	Access to accountable REV services shall be granted to authorised voters only.	The standard requirement that limits access to those who have been properly authorised.
2.2	Access to accountable REV services shall require the presentation of an authentication credential issued by or on behalf of the e-voting registration service.	An implementation will require that the registration service provide a suitable authentication token.

A.5.3 OS3 – Effective Voter Anonymity

3.1	The REV service will not be able, under normal operation, to associate the identity of the voter with their recorded vote.	Any voting system must support the voters' right to secrecy of their vote, under normal conditions. Hence the vote recording mechanism must not identify the individual voter.
3.2	The REV service will, after judicial instruction, make available such data to determine votes with the associated identity of the voter.	The REV service will enable a third party under judicial instruction, probably the Electoral Commission, to establish the identity of a voter in order to investigate any claims of fraud or gerrymandering.

A.5.4 OS4 – Effective Vote Confidentiality

4.1	The REV Service shall provide the voter with an effective method of ensuring the confidentiality of the vote when it is communicated.	Effective end-to-end encryption may be required to protect the vote from disclosure to third parties during transmission. Alternative methods such as the use of random assigned voting numbers also provide the same facility.
4.2	The REV Service shall ensure that data relating to the vote cast will not persist on the client machine, potentially undermining vote confidentiality.	After the vote has been cast if there is a requirement for the voter to receive feedback on how they voted. Direct evidence of how the vote was cast must not be sent to the client system, as storing direct data could compromise the confidentiality of the vote or enable

		coercion to take place.

A.5.5 OS5 – Effective System Identification and Authentication

5.1	Access to the REV system will be granted to authorised administrators and operators only.	The standard identification and authentication requirement to limit access only to those who have been properly identified and authenticated.
5.2	Administrator and operator privileges shall be the minimum necessary to satisfy the operational requirements for the REV System.	A standard privilege minimisation requirement to limit the potential damage caused by authorised administrators and operators.
5.3	It is desirable that access to the REV System be conditional upon presentation of an access token issued by or on behalf of government services providers.	Access control can be made stronger through the use of properly designed access tokens. For the REV System the extra security afforded by access tokens could justify their provision.
5.4	Administrator and operator access shall require the presentation of authentication credentials and supporting information to identify the individual requesting access.	An implementation requirement for personal authentication beyond possession of a token. The method would probably be a password, perhaps in conjunction with biometrics.

A.5.6 OS6 – Effective System Registration

6.1	Administrator and operator access rights to the REV System shall be granted only when the Presiding Officer is satisfied that the user is actually who he/she claims to be, and has a legitimate need for access.	Access to the REV needs to be controlled by the Presiding Officer, or a person of similar authority. Records of those who have access to the system need to be kept for auditing and accounting purposes.

A.5.7 OS7 – Effective System Access Control

7.1	Administrator and operator access will be limited to those REV System assets and services that are necessary to support the e-election system.	A requirement to enforce internal access controls at the object or application level such that legitimate administrators and operators, once granted system access, are limited in the amount of damage to the system they can cause.

A.5.8 OS8 – Information Integrity

8.1	The REV Service shall provide the information transmitted across public networks with adequate protection from exploitation by accidental or deliberate modification, deletion or replay.	A requirement for strong communications integrity measures to prevent an attacker from manipulating the data in transit or from loss and corruption caused by equipment or communications failures.

8.2	The REV Service will protect information stored within the unassured client domain from exploitation by accidental or deliberate modification.	A requirement to ensure that the operating system and application used to access the REV Service are free from malicious code that could undermine the integrity of the vote.
8.3	The REV System shall protect information transferred within the implementation domain from accidental loss or corruption.	A requirement for ‘best practice’ integrity measures within the system. This will also lead to a requirement to implement appropriate backup measures.

A.5.9 OS9 – Service Availability

9.1	The REV Service shall be protected against outside attack, which seeks to damage or deny provision of the service to voters.	A requirement for strong security measures to prevent the service being susceptible to external denial of service attacks.
9.2	The REV Service will be protected against internal equipment failure, which might damage or prevent continuing provision of the service.	A requirement for best practice design approaches to prevent the service being unduly susceptible to unavailability following equipment failure. This will require a measure of redundancy consistent with the importance of continued service provision and the ability to effect swift repairs.
9.3	The REV Service shall be protected against loss of data, loss of equipment, and other external adverse events.	A requirement for a business continuity plan and supporting measures. There is a general requirement to anticipate disasters and make sure that the necessary measures are instituted to avert the disaster where possible and recover where prevention is not an option.

A.5.10 OS10 – Information Availability

10.1	The REV Service shall make the provision for the retrieval of voting or relevant registration information that has been damaged or destroyed by malicious or other actions.	This is a business continuity requirement for a proper backup regime to ensure that the active datasets are secured and can be restored in the event of failure.

A.5.11 OS11 – Service Protection

11.1	The REV Service application and underlying network infrastructure shall be protected against outside attack that seeks to undermine continued service provision.	Any system that is connected to public networks is open to attack by those seeking to damage or deface the service without necessarily seeking personal gain. The underlying networks must be hardened against such attack using measures such as boundary control and scanning devices. The applications themselves must be constructed in such a

		way that vulnerability to outside attack is reduced to an acceptable level.

A.5.12 OS12 – Operator Integrity

12.1	The REV System shall be operated and administered by trusted individuals.	Individuals administering and operating, and those individuals who operate in close vicinity to, any service provision equipment should either be 'vetted' or two-man rules should be in operation. 'Vetting' in this context may not require formal security clearances, but some form of background checks, especially for political subversion etc, is required.

A.5.13 OS13 – Open Auditing and Accounting

13.1	The REV System providers shall maintain a comprehensive record of transactions and system events that will be available to an independent body overseeing the election for purposes of analysis. This must also be available after the event	General requirement for maintenance of audit and accounting logs. Reasons for requiring this include establishing accountability for transactions and furnishing evidence in the event of a dispute about the REV service.

A.5.14 Assurance

99. It is difficult to determine how much assurance is required in an implementation before it can be allowed to go live. Assurance can be expressed in terms of levels, known as EAL, using an internationally recognised system called the Common Criteria (indeed, this requirements expression has been determined through the use of the CC). The higher the level, the more assurance can be had in the correct implementation of system functionality.

100. However, the more assurance required, the more expensive that assurance becomes. Commercial best practice tends to deliver products at or about EAL4.

101. The UK operates a number of schemes that provide confidence in the implementation of a particular product or system. Two of these schemes would be relevant to e-Voting system assurance:

   - full Common Criteria Evaluation to say EAL4, which would in turn require:
     - Common Criteria Protection Profile to be developed for e-Voting systems in general;
     - each implementation to develop a Security Target mapping Security Enforcing Functionality on to the Protection Profile;
     - each implementation to under go an evaluation assessing whether the implementation of the security target has been met with sufficient rigour.
   - A FASTTRACK assessment, which aims to achieve very significant cost and timesaving compared to most formal evaluations, and to be sufficiently widely applicable to be a genuinely useful addition to the range of assurance

options available. The main characteristics of the Fast Track Assessment (FTA) Service are:

- tailoring (and relaxation) of many formal evaluation requirements to address the specific product/environment;
- an underpinning of Common Criteria principles used in formal evaluations, so that assurance statements can be related to National Infosec Policy (HMG IS1);
- a cost and/or time-limited process, based on prioritised evaluation activities;
- increased interaction between the Developer of the product and the Assessor;
- more sampling of evidence than permitted in formal evaluations;
- emphasis on functional and penetration testing to find errors and vulnerabilities;
- it is a one-pass service;
- there is no formal assurance level awarded;
- there is no assurance maintenance as the results are tailored to specific system requirements.

102. The UK is also developing a FIPS-140 evaluation laboratory, which is aimed at assessing cryptographic components of systems and products.

103. Other forms of assurance exist of course. The Open Source philosophy of peer review is another method (if not entirely formalised), as is contracted independent scrutiny.

Annex B. Background Review

B.1 Introduction

> *"One of the primary motivations that has been given for remote Internet voting is the possibility of increased voter turnout."*
>
> *Dr. Lorrie Faith Cranor*

104. Voter turnout has been in steady decline for a number of years and in the last General Election (2001) it was down to 59%. There is particular cause for concern regarding the turnout among 18-24 year olds, estimated at just 39% in the 2001 General Election.

105. The UK Government is keen to increase public engagement across the political process. Inconvenience is a barrier to voting, and the Government is satisfied that there is a prima facie case for implementing Remote Electronic Voting (REV) to provide flexibility and choice in voting methods.

106. The high profile political interest in online voting is creating the demand for a workable solution in the near future; however there are many unresolved issues with regard to the security of solutions and their ability to maintain the integrity of the election process. It is important that these issues should not be sidelined in favour of a speedy implementation.

107. In the recent UK Local Elections 2002 it was reported that there was an average increase in turnout of 4%; in constituencies where Internet Voting was piloted, the additional increase in voter turnout was only 1%. However this figure is not particularly meaningful as trials were only conducted in a small number of wards and does not capture the use of Internet voting in preference to other methods.

B.2 Purpose and scope

108. This annex is intended to provide a background on what has happened to date with regard to remote electronic voting (REV). It is not intended to be a technical document per se and avoids in-depth discussion of specific protocols.

109. The annex identifies prominent academics, academic projects, authentication techniques, previous and planned implementations and standards bodies, and identifies key points based on the experience and opinions of the sources. From the key points a set of recommendations is outlined to facilitate the adoption and introduction of Online Voting.

B.3 Definitions

- **electronic voting (or e-voting)**: any voting method where the voter's intention is expressed or collected by electronic means.
- **electronic counting**: technologies that electronically count physical ballots, such as optical scanning of ballot papers.
- **kiosk voting**: in the electronic context, kiosk voting means the use of dedicated voting machines in polling stations or other controlled locations. Voters mark their choice electronically (perhaps on a touch sensitive screen) rather than on a paper ballot. The votes are counted on individual machines, known as Direct Recording Electronic (DRE) machines, and the votes cast are transferred to the central tallying point by unspecified means. A ballot

paper can be printed and retained in confidence in a ballot box as an additional check.

- **remote electronic voting (REV)**: this is the preferred term for voting that takes place by electronic means from any location. This could include the use of the Internet, text message, interactive digital TV, and touch-tone telephone.
- **online voting**: taken literally this means voting in an electronic way while connected to a live system. It therefore includes not just REV, but also forms of Kiosk voting where there is a permanent connection to a central server.
- **Internet voting (or i-voting)**: A specific case of Remote Electronic Voting whereby the vote takes place over the Internet such as via a web site or voting applet. Also sometimes used synonymously with Remote Electronic Voting. That usage is deprecated, and the term will instead be used to refer to a strict subset of REV.
- **online election system**: the physical system responsible for handling the online election process.
- **client**: the device which the voter uses to interface with an online election system
- **voting server**: a generic term for a server component of an online election system.
- **personation**: the act of fraudulently voting in someone else's name.

B.4 Prominent Academics

> *"At least a decade of further research and development on the security of home computers is required before Internet voting from home should be contemplated."*
>
> *Professor Ronald Rivest, MIT [14]*

110. Following the 2000 US Presidential Elections problems with some voting methods came to the fore in the US. This sparked an interest in academic circles with the regards to the security of electronic voting systems, with particular interest in Internet voting, which the public was beginning to regard as a viable voting solution. Some prominent academics in the field of information security provided statements on Internet Voting to public bodies within the United States. The following is a brief appraisal of some prominent academics and their opinions with regards to Internet voting.

B.4.1 Dr. Lorrie Faith Cranor

111. Dr. Cranor has done a lot of research on electronic voting and as part of her Master's degree at the University of Washington, she proposed protocols that were implemented in the Sensus Project; a security conscious Electronic Polling system for the Internet. Currently she is working for AT&T Research Labs and has been involved in designing the technical aspects of an electronic voting system trial for Costa Rica.

112. Dr. Cranor has a practical view on electronic voting; in an ACM Crossroads article, "Electronic Voting: Computerized polls may save money, protect privacy" [Reference 7], she highlights one of the most significant issues of electronic voting:

> *"simultaneously achieving security and privacy in electronic polls is a problem that must be solved if the Internet is to be used for serious large-scale surveys and elections."*

B.4.2 Dr. Rebecca Mercuri

113. Dr. Mercuri currently works for Bryn Mawr College, Pennsylvania and has been involved with Electronic voting since 1991. Her thesis: 'Electronic Vote Tabulation Checks & Balances' was submitted for her Ph.D. at the University of Pennsylvania on April 30, 2001 [9].

114. Dr. Mercuri takes a very cautious view with regards to implementing electronic voting systems and considers Internet Voting to be a highly inappropriate voting method. To that effect, on her web site, she categorically states:

> *"I am adamantly opposed to the use of any fully electronic or Internet-based systems for use in anonymous balloting and vote tabulation applications". [8]*

115. In her thesis Dr. Mercuri draws the following conclusions:

    - computer-based voting offers increases in the rate at which votes can be processed in exchange for a variety of risks that are either not present or greater than those in manual balloting systems;
    - problems with electronic voting systems such as large-scale fraud, denials of service and the incompatibility of anonymous voting with audit trails, are inherently not resolvable;
    - remote Voting systems are particularly vulnerable to the above attacks as well as problems such as vote selling and coercion and should not be used at all;
    - wherever possible, voter authentication, ballot casting and vote tabulation should be provided in separate systems;
    - purely technological solutions fail to adequately address the sociological issues inherent within the democratic election process. Voting systems must require the inclusion of human checks and balances as a necessary implementation component;
    - DRE-style-devices may offer the best potential compromise for vote casting since they can provide human-verifiable printed ballots that can be used in the case of recounts; and can be security-hardened and self-contained.

116. Although these conclusions are not conducive to a practical implementation of Internet Voting they highlight issues to consider.

B.4.3 Dr. Peter G. Neumann

117. Dr. Neumann is a prominent risk expert working for Stanford Research Institute in California. He is the moderator for the ACM Risks Forum and has written numerous articles on risks associated with Internet Voting Systems. In one such article he states:

> *"the shining lure of these "hype-tech" voting schemes is only a technological fool's gold that will create new problems far more intractable than those they claim to solve".*

118. Dr. Neumann believes that an intrinsic lack of security in Internet systems and a morass of sociological problems limit Internet Voting; these issues are discussed later in greater depth.

119. In a paper entitled “Security Criteria for Electronic Voting”, [11], he proposes a generic voting criteria, outlined below:

- system integrity: the computer systems used in the voting process must be tamperproof;
- data integrity and reliability: votes must be recorded correctly;
- voter anonymity and data confidentiality;
- operator authentication: all people authorized to administer an election must gain access with nontrivial authentication mechanisms;
- system accountability: all internal operations must be monitored, without violating voter confidentiality;
- system disclosure: the system software, hardware, documentation, microcode, and any custom circuitry must be open for random inspection at any time, despite cries for secrecy from the system vendors;
- system availability: protection against denial of service attacks;
- system reliability: system development (design, implementation, maintenance, etc.) should attempt to minimize the likelihood of accidental system bugs and malicious code;
- interface usability;
- documentation and assurance: the design, implementation, development practice, operational procedures, and testing procedures must all be unambiguously and consistently documented;
- personnel integrity: people involved in developing, operating, and administering electronic voting systems must be of unquestioned integrity.

B.4.4 Dr. Bruce Schneier

120. Dr. Schneier is a renowned cryptography and security expert and has written a number of major texts on the subjects. He is the author of the book “Applied Cryptography”. Dr Schneier is a Founder and the Chief Technical Officer of Counterpane Internet Security, Inc.

121. Dr. Schneier asserts that encryption provides no assurance of privacy and accuracy of ballots cast as even strong cryptographic systems can be hacked. He says:

> *“[an Internet Voting System] would be the first secure networked application ever created in the history of computers.” [12]*

122. Dr. Schneier however, maintains a pragmatic view of Internet Voting. He believes that there is a need to maintain a paper trail of the votes cast without revealing how individuals voted, for use in case of a recount.

B.4.5 Professor Ronald Rivest

123. Professor Rivest of MIT (Massachusetts Institute of Technology) is a respected academic in the field of Information Security; he is the co-inventor of the popular public key algorithm- RSA.

124. Professor Rivest holds a more balanced view on electronic voting than his peers and has proposed four specific security-related recommendations, which were submitted to the CalTech/MIT VTP Press Conference July 2001 [13]. These were:

- move away from monolithic voting structures;
- maintain a physical audit trail of results. This audit trail should be directly created by the voter, or at least be directly verifiable when a vote is cast. Many proposed US electronic voting systems fail this requirement;
- make the security critical source code for the vote-recording and vote-counting components "open source". Rivest argues that this will increase public confidence in the election system;
- delay Internet voting (voting from home) until fundamental security issues, such as the security of the underlying platforms (that is, of the home PC's) have been adequately addressed.

125. Although Rivest recommends that Remote Electronic Voting be delayed until there has been significant improvement in the security of home computers, he believes that electronic systems can be used to assist the current election process, for instance use in registration procedures.

B.5 Academic Projects

126. The foundation of much of the academic work in the area is a paper by Fujioka, Okamoto and Ohta entitled “A practical secret voting scheme for large-scale elections”. Practically-focussed projects build on the blind voting protocol proposed in this paper.

B.5.1 De Montfort University Review

127. This Review was commissioned by a range of agencies across central and local government, including:

- the Department for Transport Local Government and the Regions (DTLR)[1];
- the Society of Local Authority Chief Executives (SOLACE);
- the independent Electoral Commission;
- the Local Government Association (LGA);
- the Improvement and Development Agency (IdeA);
- the Association of Electoral Administrators (AEA);
- the Office of the e-Envoy (OeE).

128. The Review is written on the premise that Remote Electronic Voting (REV) will be introduced at some point in the future. To that effect, it considers potential barriers to implementation and gives recommendations to facilitate implementation. The focus of the Review is broad, covering technical, legal, political, organisational and socio-psychological aspects associated with online voting.

129. The three major barriers to implementation identified in the Review were:

- **secrecy**: the UK is signatory (or at least normatively bound) to a number of international declarations and protocols, that require voting to take place in secret. The Review claims that the legal issues would not be too difficult to address; however the issue of public confidence would require some degree of public education and consultation;

[1] Responsibility has since passed from DTLR to the Lord Chancellor’s Department and the Office of the Deputy Prime Minister.

- **security**: the Review acknowledges that the security of the technology is a significant barrier to implementation of REV;
- **technology penetration**: voter capacity to use the technology is a significant barrier to adoption of REV. The Review states that there needs to be widespread public use of any technology prior to its adoption as the basis of a REV.

130. Some interesting recommendations from the report were:

- the introduction of online voting is seen as a long-term goal;
- the security of the voting system should not be compromised in favour of speedy adoption. However, during implementation some trade-offs will have to be made;
- the Voting System should not be centralised, ensuring that there is no single point of attack and increasing operational flexibility in terms of user interfaces chosen;
- a multi-channel approach (a combination of Internet, interactive digital TV, telephone etc.) should be taken to REV, is in recognition of technology penetration issues.

B.5.2 Caltech - MIT/Voting Technology Project

131. The Massachusetts Institute of Technology and the Californian Institute of Technology are undertaking a joint project on the subject of electronic voting techniques. This Project is an intellectual exercise rather than implementing any solutions. It pools the technical and socio-political expertise of the two institutions.

132. The Project has produced a paper entitled “Voting - What is, What Could Be” [15] the main conclusions of which are as follows:

- integrity of absentee balloting is a real concern. Allowing early voting is recommended in preference to postal voting;
- remote Internet Voting poses serious security risks. The Paper recommends a delay on Internet voting until suitable security criteria are in place;
- the US Federal government must create and fund a system for evaluating equipment based on lab and field-testing of equipment;
- audits of equipment should be conducted even when there is no requirement for a recount.

B.5.3 Workshop on Election Standards and Technology (WEST) 2002

133. WEST is a small research-oriented workshop organised by the Caltech-MIT Voting Technology Project and Dr. David Chaum. The project is devoted to examining election standards and technology. The workshop is funded in part by the National Science Foundation and hosted by the American Association for the Advancement of Science.

B.5.4 MIT E-VOX system

134. A project at MIT under the supervision of Professor Ronald Rivest culminated in an Online Voting (at least partial) solution called E-VOX. This was the result of work carried out by Mark A. Herschberg at MIT [6].

135. E-VOX has been implemented using Java, Netscape and JDBC (Java Database Connectivity). The system is still involved in teaching and research and was used for an Undergraduates Association election at MIT in 1999.

B.5.5 The Sensus System

136. As part of Lorrie Cranor's thesis she developed a project called "Sensus: A Security-Conscious Electronic Polling System for the Internet" [5], which uses blind signatures and distinct entities for counting and verification.

137. The project has fallen by the wayside since she graduated, and on her website Dr. Cranor expresses a preference for MIT's EVOX project. Citizens of the US and Canada can download the C and Perl source code from her website.

B.6 Authentication Techniques

B.6.1 The Voting Process

138. The voting process can be separated into two actions: registration and voting. At the registration stage voters must identify and authenticate themselves to a registration authority. Any individual able to vote will then receive some a set of credentials that will be used to verify the individual immediately before the vote takes place.

139. If before voting this second set of authentication and identification details are not accompanied by additional authentication techniques (for example, personal recognition in polling stations) then the overall authentication of the system is only as good as that of the registration process.

B.6.2 Registration Authentication Techniques

B.6.2.1 In Person

140. The US DoD Federal Voting Assistance Program required that voters register in person to a Local Registration Authority or an appropriate agent, and present photo identification.

141. The advantage of face-to-face registration is that it has a level of authentication that is as good as that required to obtain the photo identification.

142. The disadvantages are that the cost of face-to-face registration precludes it being used on a national level, and that the inconvenience to the voter is high.

B.6.2.2 By Mail

143. The current system in the UK enables voters to register by mail; by signing to say that their name and address are correct and then having a third party validate their credentials and signature.

144. The advantage of this is that the cost per voter is much lower than that of in-person registration and that it is much simpler for the voter to do.

145. The disadvantage is the ease of faking the authentication (the signatures), if the signatures on the registration document are not compared with actual signatures. This was highlighted when a team of BBC investigative journalists was able to obtain a postal ballot, using the names of deceased citizens.

B.6.2.3 Over the Internet

146. Masquerading on the Internet is a trivial exercise as the recent spate of adults impersonating children online, for nefarious reasons, has highlighted. Considering a number of techniques for authentication is a useful exercise.

147. The current de facto method of online authentication is the use of passwords, but this relies on the individual already having an ‘account’ to the server; obviously this is no use as a method for registration.

148. A suggested system uses a back-end database comprising of the electoral roll. The user provides name, address and other details, which are then compared with the database. If the user is eligible to vote she is prompted to choose a password, then issued with a unique identification number via email, along with a link to the voting web site. In this case, the credentials used to authenticate the voter to the voting server before voting have a good level of authentication; however, no authentication is required to obtain them. Hence, overall there is no authentication required to vote. All one would need to do in order to register and vote fraudulently is to obtain a list of names and addresses in the area.

149. A possible method of online registration in the future is to use pre-existing digital certificates. To be effective however, this would require a national Public Key Infrastructure (PKI). If the certificate is to be trusted a registration method requiring strong authentication such as face-to-face or multiple signatories, is required. Once again, if a certificate was obtainable online, the authentication would be too weak for the certificate to be trustworthy.

150. The advantage of registration on the Internet, sometimes referred to as I-Registration, is that it potentially incurs a very small incremental cost.

151. The major disadvantage is that there is currently no way of implementing feasible authentication mechanisms.

B.6.3 Voting Authentication Techniques

B.6.3.1 PIN, Passwords and Virtual Ballots

152. This is the simplest and most popular method used for identification and authentication of voters and was used during the 2002 Local Elections in Sheffield and Liverpool.

153. A possible implementation of the PIN and password system is to distribute cards, via post or hand, containing the two pieces of information and a link to the site where the voter can cast a vote. The voter then goes to the specified site and enters the details on the cards. This authenticates the voter to the voting server and presents a virtual ballot paper on which they select their preferred candidate.

154. This system requires that the PIN and password remain secret before the election and that end-to-end encryption such as SSL is used between the client and voting server.

155. The advantages of this system are the ease of use by the voter and the fact that the cost of distribution would only be marginally more than existing voting cards.

156. The principle disadvantage is that, assuming that the both of details are compromised and there are no other methods of authentication before voting, the voter can be personated . Vote selling is also possible. To reduce unauthorised disclosure of these details, a scratch-off panel could be added to the cards; the voter would then know if the details had been compromised.

B.6.3.2 Digital Signatures and Virtual Ballots

157. A digital signature can be assigned to the user after registration has been completed. Each digital signature has an associated private key. It is essential that this private key remains in the sole possession of the voter and is protected by a strong password. It is possible to generate the key on the client machine but in some circumstances it may be preferable to generate it on the voting server; this creates a need to consider distribution methods.

B.6.3.3 Hardware Tokens

158. The US DoD Federal Voting Assistance Program used a floppy disk to store the private key and secured it with a password. Other standard media alternatives include CD-ROM, USB tokens, and even DVD.

159. The EVOX project at MIT used iButtons: small devices with up to 134Kbytes of physically tamperproof memory that holds the password-protected private key and will record when and where the key is accessed. These require a special reader and are less appropriate for the average remote user, and were in fact used for bespoke remote voting clients under control of the election officials.

160. The main advantage of providing these tokens is that possession of the token is required in order to vote. Hence if the voter possesses the token and the password remains secret, they can assume that nobody has voted in their place.

161. The main disadvantage of providing these tokens is the cost of production and distribution.

B.6.3.4 Soft Tokens

162. A soft token - essentially a file on disk - would contain the private signing key. This would be present on the client's system and protected by a client-chosen password. It should be stored nowhere else.

163. Some current systems use a soft certificate. The private key can be generated on the server and sent using SSL, or a similar transport layer security protocol, to the client, or it can be generated on the client side

164. The main advantage of using soft tokens is that the marginal cost per certificate is very low.

165. The main disadvantage is that the soft tokens are more open (than hard tokens) to duplication, and hence masquerading.

B.6.3.5 Digital Profile

166. A digital profile is essentially a private key stored on the server, normally protected by a PIN and password authentication mechanism. To the user and attacker this would appear identical to the PIN and password mechanism.

B.6.3.6 Cryptographic Strings

167. One company uses a six-character identification code called a CADC (compact anonymous digital certificate). This is given to the user along with a password and can be used from anywhere. When the user logs on, the voting system has no prior knowledge of the CADC or the password, yet can authenticate the voter and determine which ballot the voter is to see from the information given.

168. Another possibility is to use a pre-pay mobile phone top-up card analogy in which a voter is provided with a 16 digit number that contains their identity,

constituency and who they wish to vote for, but as a result of encryption these details cannot be derived from the number alone. This number would be accompanied by a password.

B.6.3.7 Mobile Telephones and SIM cards

169. It is possible to use the SIM card in a mobile phone as a hardware token and PIN. This is used in conjunction with an Internet browser to authenticate an individual. This method was invented with a view towards e-Business services, and has not been tested with online voting.

B.7 Previous and planned implementations

170. This section looks at previous implementations in the UK and world-wide.

B.7.1 UK

171. Before the Local Elections of 2002, Online Voting had only been used for local referendums and did not give very encouraging results. In the London Borough of Islington just 2.4% of the votes were cast via the Internet, and 2.3% used telephone voting.

172. There were also online voting trials conducted in Bristol and Croydon where the percentage of voters using the Internet was 2.7% and 3.4% respectively.

173. St. Albans, Sheffield, Liverpool are some of the constituencies that enabled their voters to use online voting methods in the 2002 local government elections. As mentioned in the Introduction, the increase in voter turnout in constituencies using Remote Electronic Voting was just an additional 1%. This is compared with a national average increase of just over 3%. These figures should not be considered conclusive, although turnout did not increase significantly, individuals did choose to vote online instead of using traditional methods. As with any new idea, take-up is not immediate.

B.7.2 Europe

174. In September 2000 the EU Commission established a ‘Cybervote Project’ it was granted Euro3.2m over the next 3 years to demonstrate a highly secure cyber-voting prototype using mobile and fixed Internet technologies. The project officially started on 1 September 2000 and will end 1 March 2003. Trials will be held in Krista/Stockholm, Issy-les-Moulineaux and Bremen. The project website hosts useful technical papers for Internet voting and can be found at the address: www.eucybervote.org.

175. The Netherlands has established its own ‘Remote Voting Project’. It will experiment with Internet Voting from any polling station of the voter’s choice and from special public ‘voting columns’ in the Provincial Elections on 11th March 2003.

176. Estonia has changed its law to allow Internet Voting in all elections. This will be piloted in the 2002 local government elections, and if it is successful the system will be rolled out for the Parliamentary Elections in 2003.

B.7.3 The California Internet Voting Taskforce

177. The California Internet Voting Taskforce believes that despite numerous challenges, it is technologically possible to utilise the Internet to develop an additional method of voting that would be at least as secure from vote-tampering as the current absentee ballot process in California.

178. The California Internet Voting Task Force was established to make Internet Voting a reality in California. The Task Force has published a report on the Feasibility of Internet Voting dated January 2000 in which it recommends that Internet Voting be introduced incrementally in the short-term rather than comprehensively. To that effect, the report outlines a pragmatic approach to implementing online voting, suggesting four stages for the introduction of Internet Voting.

179. The four stages are:

- Internet voting machines used in traditional polling places;
- voter may cast ballot on any county controlled Internet voting machine. election officials are present for voter authentication;
- voter authentication code provided by elections office allows voters to cast ballots at any county-controlled internet voting machine;
- voter authentication code provided by elections office allows voter to cast a ballot from their own home or office computer.

180. Alongside the incremental approach, the Task Force recommends that Internet Voting is not implemented as a complete replacement to traditional voting systems and that the adoption process is modelled on the California absentee ballot process.

B.7.4 US DoD Federal Voting Assistance Program

181. The US DoD Federal Voting Assistance Program released a report [Reference 17] on a pilot project for voting over the Internet. This was piloted for Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) voting during the November 2000 Presidential Elections. 84 citizens used the system and its existence was not highly publicised which mitigated outsider attacks on the system.

182. Overview of the system:

- registration involved personal appearance in front of a Local Registration Authority, or trusted agent, with official photo identification;
- authentication to the voting server was achieved using password-protected digital certificates that were issued using the Medium Assurance DoD PKI. These were distributed using floppy disks. The individuals were added to an access control list that was used to limit access to the E-Ballot tool server;
- before the individuals could vote they had to install a furnished browser and custom plug-in application from a CD-ROM, delivered via commercial carriers. The system used Windows 95/98 and Netscape Navigator.

183. The pilot system was compared to the current UOCAVA postal system and the report claimed that for the Internet voting system the authentication and identification were superior to the postal system. This was due to the use of a PKI infrastructure and face-to-face registration. This type of implementation is not currently feasible on a national level due to lack of a supporting public key infrastructure.

184. Expansion of the voting system is to use a low-risk incremental approach, eventually phasing out the distribution of CD-ROMs, containing the ‘clean’ operating system and browser, by mail and moving to a secure voting process online.

B.7.5 Standards Bodies

B.7.5.1 OASIS

185. The Organisation for the Advancement of Structured Information Standards (OASIS) is currently active in writing an extension for XML, Election Mark-up Language (EML). This is an XML specification intended for the structured interchange of data among hardware, software and service vendors who provide election and voter services.

186. The UK government is heavily involved with OASIS's EML activities. There is a committee called the OASIS Election and Voter Services Technical Committee of which the Office of the e-Envoy is an active member.

B.7.5.2 Administration and Cost of Elections (ACE) Project

187. The ACE project comprised of three organisations:

- the Institute for Democracy and Electoral Assistance (IDEA);
- the International Foundation for Election Systems (IFES);
- the United Nations Department of Economic and Social Affairs (UN-DESA).

188. The site www.aceproject.org provides a good background on all aspects of electronic voting from election legislation voting technology.

B.7.5.3 United States Federal Election Commission

189. The US Federal Election Commission (FEC) produces guidelines for the running of US elections, called Voting System Standards (VSS). In 2001 the VSS stated:

> *"at this time…the VSS do not promote Internet Voting"*

190. FEC also state:

> *"the Standards allow for Internet voting systems operated in parallel with another voting system, and do not address or allow for stand-alone Internet voting systems."*

191. It is apparent that the Commission are planning to phase Internet Voting into the guidelines in the near future, an indication that Internet Voting is likely to be adopted in the US at some point.

B.7.5.4 Open Source Community

192. Some US academics recommend the use of open source solutions in e-voting. This has advantages when it comes to public confidence in the system, as the De Montfort Review pointed out, and will help to reduce the number of proprietary solutions that could potentially flood the market.

193. Within the GNU open source community there is an e-democracy project to create a GNU.FREE Internet Voting System. This is implemented using Java and XML. A member of the project has been involved with meetings with the OASIS Election and Voter Services Technical Committee meetings.

B.8 Key points

B.8.1 Current Voting Systems Vulnerabilities

194. The current polling station and postal voting systems have vulnerabilities.

B.8.2 Client Platform Vulnerabilities

195. Clients that are connected to the Internet can potentially be attacked from anywhere in the world. Furthermore, current operating systems and browsers are insecure, as past events such as the ‘I LOVE YOU’ virus have demonstrated.

196. The following are some examples of possible attacks on the client that can undermine the confidentiality and integrity of the vote and in some cases the availability of the system.

B.8.2.1 Trojan Horses

197. A ‘Trojan Horse’ can be installed on the client’s machine and will appear to the user to be doing one thing and in fact be doing another. For example: the user may think that they have voted for Alice when in fact the program has cast a vote for Bob; undermining the integrity of the vote. There are also confidentiality issues as the program could simply send the information to a malicious Internet host.

B.8.2.2 Viruses

198. Viruses can infect the client machine well before the date of an election and remain undetected on the client machine until the day the election begins at which point they are activated. A virus could result in a denial of service (DOS) attack, as the voter would not be able to use the affected client to vote.

B.8.2.3 Domain Name Server Attacks

199. The DNS lookup tables can be altered just before the election so that when a client attempts to access the voting website, unbeknown to the voter it actually points to another website run by a malicious group who intend to steal votes or prevent votes being cast.

200. It is also possible for a nefarious program to alter the proxy settings in the browser so all of the web transaction of the client went via a certain site. It is not possible for a secure connection to be made with the voting site using this method; however the proxy server can establish a secure connection with the client and make it appear bona fide.

B.8.2.4 Social Engineering Attacks

201. Some of the attacks above rely on the simple art of persuasion, essentially capitalising on user’s lack of understanding of the system they are using. This highlights the need for effective user education before launching an online voting system.

B.8.3 Centralised Voting Systems have vulnerabilities

202. Professor Ronald Rivest suggests that we move away from monolithic voting structures. However employing many online voting systems would be costly and could lead to inconsistent implementations. The problems associated with a centralised system are as follows.

B.8.3.1 Single Point of Attack

203. Although a voting server can be hardened using the latest security techniques, it is still open to the same sorts of problems as those that were highlighted for client vulnerabilities.

204. The information is also stored centrally in electronic format so in theory it is easy to copy and manipulate.

B.8.3.2 Greater Potential of an Insider Attack

205. Since the volume of information available on the system is greater it is more valuable and hence more vulnerable to an attack from an insider. For a centralised system Election Officials would need to be vetted before assuming the role.

B.8.3.3 Mass Attacks on the Infrastructure are Possible

206. The communications infrastructure is the link between the client and voting server. It is possible that an attacker could mount a denial of service attack on the Internet routers on the day of an election and deny the use of the online system. Another possibility is to use up a large amount of bandwidth on the voting server.

B.8.4 Remote Voting has Inherent Vulnerabilities

207. Remote voting is a new area and presents vulnerabilities that did not exist in previous voting systems.

208. Dr. Rebecca Mercuri sums up the problems with Remote Internet voting eloquently:

> *"off-site Internet voting creates unresolvable problems with authentication, leading to possible loss of voter privacy, vote-selling, and coercion."*
>
> *Are you saying that you agree that the problems are unresolvable – if not, this should be made clear! I agree.*

B.8.4.1 Online Registration has No Feasible Methods of Authentication

209. Online authentication for registration purposes is not feasible without the use of an infrastructure, such as a PKI. Hence electronic registration must be used in conjunction with a secondary voting authentication process that ensures that it is hard to personate another individual.

210. Although registration is not suitable without a supporting PKI, online voting can be made at least as secure as the existing postal voting system.

B.8.5 Privacy Issue

211. It is a right of voters to have their ballot kept secret; however they also need feedback in order to verify that the vote they have cast is correct. In a remote environment it is possible for a third party to verify how an individual voted. Hence the voter is open to coercion of their vote.

212. Although over-the-shoulder observation is more of a social problem, technical measures can be taken to ensure that there is no persistent trace of how an individual voted on their electronic device. For example for Internet Voting it should be ensured that persistent cookies are not stored on the computer and there is no trace of persistent information anywhere on the hard drive that would betray the vote.

B.8.6 Audit Trail vs. Anonymity

213. Academics highlight the need to maintain a paper trail of how each individual voted, for the case of the votes needing to be manually counted in the event of a recount. The presence of such an audit trail will mean that an individual can be traced back to their vote, compromising their anonymity. There will always be a trade-off between the two.

B.8.7 System Design is an Important Issue

214. The design of the systems used for online voting is essential to their security. The following categories are important considerations in the design of online voting systems.

B.8.8 Assurance Criteria are Formalised

215. In her thesis: "Electronic Vote Tabulation: Checks and Balances" [Reference 9], Dr. Mercuri proposes that assurance criteria are agreed upon and enforced for electronic voting systems. To that effect she outlines some generic security assessment questions in conjunction with the Common Criteria components. Application of such assurance standards would ensure that voting systems reached a minimum acceptable security standard before being deployed.

B.8.9 Standards

216. This would facilitate interoperability between solutions and clients and avoid one company's solution being dominant in the marketplace, which would be dangerous from a security point of view as vulnerabilities would be widely known and publicised. Standards would also reduce the amount of proprietary voting solutions that would emerge without the use of standards that would also create problems with keeping the systems secure.

B.8.10 Disclosure of Security Critical Code

217. Professor Ronald Rivest recommends that the security-critical component of an online voting system be open source. This may be a step too far however, certainly companies providing REV solutions should expect to disclose the source code to the election authorities, in order to ensure to have an independent review of the security of the system.

B.8.11 Documentation of the System

218. Documentation is essential to solid design and maintenance of an online voting system. Dr Neumann states:

> *"the design, implementation, development practice, operational procedures, and testing procedures must all be unambiguously and consistently documented."*

B.8.12 Usability

219. The usability of the system is not just a social issue. If the interface is badly designed then a voter may cast the vote for the wrong candidate as was claimed to be the case in Florida's Palm Beach County Presidential Election 2000, for the infamous 'Butterfly-ballot'.

220. In the case of a voter making the wrong choice of candidate for whatever reason, there could be an intermediate step where a confirmation is required and if the vote was cast incorrectly the option of rolling back the vote is offered. Alternatively the usability of the system should be good enough for such occurrences to be sufficiently unlikely.

221. Different implementations for different voting channels should be avoided. This would perhaps involve limiting the input to numbers, as these tend are common to most delivery channels of interest. .

B.8.13 Online Voting is not a Panacea

222. The 1% increase of voter turnout in wards allowing Internet Voting during the 2002 UK Local Elections indicates that adoption of Online Voting will not be a miraculous process. As with all new technologies widespread public adoption will only happen over time, so there is in fact no need to rush the deployment of online voting. This is conducive to an incremental approach to introduction.

B.8.14 Current REV Assumption Should Perhaps Be Questioned

223. Some of the current assumptions for online voting systems need to be reviewed as they have somewhat limited research to date.

B.8.15 Virtual Ballot

224. An on-screen representation of a ballot paper (a ‘virtual ballot’) is much more difficult to secure than using a simple cryptographic string. This is due to the fact that an on-screen representation of the ballot paper will require trust to be placed in the computer and operating system to correctly act upon user interactions, whereas a simple cryptographic string could just be submitted by the user and not processed by the client computer.

B.8.16 Client Side Processing Power

225. For many online voting implementations and protocols some degree of processing power is required on the client platform. This however cannot be assumed to exist for devices such as mobile phones and PDAs. A high degree of flexibility in the input, and this needs user display cannot be assumed and needs to be taken into account for in implementation.

B.9 Conclusions

226. There are a number of barriers to successful introduction of a national online voting system. The principle areas requiring consideration are insecurities of the client platform, system design issues, and user education.

227. The issues outlined above cannot be solved overnight. The introduction of Online voting should be an incremental process expanding the scope only after a successful implementation.

228. Finally, the focus of Online voting methods is limited by considering the need for a virtual ballot paper and client processing power as a prerequisite. This may not be necessary in the near future.

Annex C. Possible Security Mechanism

C.1 Introduction

229. In this section we outline a technical approach that may meet the security requirements of a very large-scale election that makes use of Remote Electronic Voting. This solution does not place any trust in the client systems, as it uses pre-encrypted ballots.

230. We start by describing how the election could appear to a voter. It is worth stressing at this point that a number of options will be presented, and some parameter choices are given as illustrative examples only. The approach outlined relies on the use of cryptography to provide security in the system. Alternatively, it would be possible to substitute use the pre-encrypted ballots with pre-generated unique random numbers and the system would work in a very similar manner.

231. For this proposal, it is assumed that the electoral roll would be managed in the normal way. In fact, this Remote Electronic Voting protocol can be implemented independently of any changes in the electoral roll.

232. By default, registered voters would receive credentials for electronic voting through the post. There would, however, be an option for voters who wished not to receive credentials for electronic voting and instead have a postal ballot or only be able to use a physical polling station. It is envisaged that a smaller-than-usual number of physical polling stations would be provided for the election. Voters who receive electronic credentials would still be able to vote in person.

233. The electronic voting credentials would be in two parts:

    - A Voter Identification Number (Voter ID). This would be globally unique and might be 16 digits long.
    - A list of candidates, corresponding Personalised Candidate Identification Numbers (PCINs) and Response IDs. The PCINs could be 4 digits long and the Response IDs slightly longer at 6 digits.

234. These pieces of information can almost be thought of as almost like a credit card number and a list of several different PIN numbers. They can also be posted separately for security, just as credit cards and PINs are at present.

235. By way of example, John Doe might receive the following:

```
John Doe
Voter ID Number: 1234567890123456
```

Candidate	**Party**	**PCIN**	**Expected Response**
Alice	AliceParty	3344	000999
Bob	BobParty	4455	111888
Charlie	CharlieParty	6677	222777
Dave	DaveParty	8899	333666
Intentionally Spoilt Ballot		1100	444555

236. To vote, John has to send his voter ID number and the PCIN of his chosen candidate. For example the following might be sent as the body of a text message to the election's SMS number:

```
12345678901234563344
```

237. The selection of 3344 as the PCIN indicates a vote for Alice, so the server would respond.

```
Response Code: 000999
```

238. John would check this number against his ballot and see it is the correct response code. As 000999 is the expected Response ID from a vote for Alice, John would know that his vote had been counted.

239. Obviously in reality Voter IDs, PCINs, and Response IDs would not have the simple structure of those above. The lengths of the numbers are dictated by the size of the electorate and the number of candidates standing, but still need to be short enough to be usable.

240. By having multiple lists of PCINs, elections that allow several votes to be cast can be conducted or several elections can be conducted at the same time. In such cases, voters would send one Voter ID followed by several PCINs. The order of the PCINs could not, however, be relied upon.

241. The rest of this appendix describes the ballot generation, ballot distribution, vote casting, and vote counting procedures in detail.

C.2 Ballot Generation

242. A ballot consists of two halves: the Voter ID and the list of candidates/PCINs/response IDs.

C.2.1 Voter ID

243. The requirement for the Voter ID is that it is a globally unique number for each voter. The space of possible Voter IDs should be sufficient to make it very unlikely for someone to guess a valid Voter ID, and there should be no apparent structure to the Voter IDs.

244. It is therefore proposed to generate the Voter IDs using a keyed cryptographic hash (HMAC) of public information such the voter's unique (public) number on the electoral roll, their constituency, the date of the election and so forth.

245. The HMAC will typically produce 128 or 160 bits of output, whereas we might use only 53 bits to generate our Voter ID. Therefore we want the first 53 bits or so to be unique in each HMAC.

246. The population of the UK is about 2^26, so as a rule of thumb we need 2 x 26 bits to be likely to get unique Voter IDs. To reduce the chances of additional work resulting from a collision, we can produce the Voter IDs on a per-constituency basis (with different keys in the HMAC for each constituency.)

247. A sufficient number of unique bits of the HMAC can then be converted to a decimal number and have a checksum digit added before being securely printed onto a scratch card on pay-slip stationery and posted to the voter.

C.2.2 PCINs and Response IDs

248. The requirement for PCINs is that they are in general different for each voter. If an interceptor knew the PCINs then a different, legitimate vote could be inserted instead of the intended one. Also, the space of PCINs should be large enough that it is sufficiently hard to guess a valid one.

249. HMACs could again be used to generate the Response IDs, for example voter information and candidate details could be fed into an HMAC to produce a keyed

hash, and the first few bits of the hash used to form the PCIN and some other data used to form a secret function used to generate the Response IDs from the PCINs.

C.3 Ballot Distribution

250. It may, in time, be possible to offer the option of distributing half of the ballot electronically and the other half by post. This would likely save money. However, the basic tenet of distributing a part of the voter's credentials in such a way that computer cannot automatically cast the vote must not be broken.

251. Consider for example what could happen if the Voter ID and PCINs were distributed by email. It would then be possible to steal credentials from people's email by hacking home computers, or even to write a virus to automate voting in a particular way. Distributing credentials on paper prevents such attacks.

C.3.1 Credential Theft

252. Voter education would be required to inform people what to do if their credentials fail to turn up in the post. This would involve contacting a central help desk that would provisionally cancel the voter's ballot, and the voter would be asked to collect a new ballot personally from perhaps their local town hall.

C.4 Vote Casting

253. The basics of the ballot-casting process were outlined in the introduction and are illustrated below:

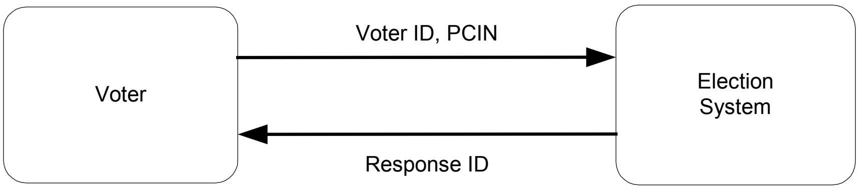

Figure 3: Basic Voting Architecture

254. Sending a vote: this requires the voter to correctly enter their Voter ID and the PCIN corresponding to their chosen candidate in order. It is assumed that some people will be unable to do this correctly first time, so procedural lockouts will be generous enough in a short timeframe.

255. The main threats to this stage are:

- identification of who is being voted for;
- modification of vote in transit;
- deletion of vote in transit.

256. The first two of these threats are met by the secrecy of the Voter ID and PCINs. It is difficult to identify who is being voted for without knowing the PCINs corresponding to a particular Voter ID. The same knowledge is required to replace a vote in transit (and if that data was known, votes could be inserted).

257. The personalised Response ID for each possible vote makes deletion of votes detectable. If a voter does not receive the correct Response ID, or any at all, she should attempt to vote again. Systems that use a generic response message are of course vulnerable to votes being deleted in transit and the generic response being spoofed.

258. From a user's perspective, this is all that is required. Due to the unreliability of some of the transport media used, such as SMS, user education will be necessary to make sure people vote again if they don't receive the correct Response ID. Similarly, the system has to be able to cope with the possibility that it was the original response that was not delivered, and that the original vote was, so people end up voting twice.

C.4.1 Multiple / Simultaneous Voting

259. Any election that allows multiple delivery channels cannot keep them perfectly in synchronisation down to the millisecond. Traditional UK elections side step this problem by denying physical votes to people issued with postal ballots. Such an approach would not be possible for an election that allows voting by text-message, Internet, touch-tone phone, interactive digital TV, and voting in person.

260. The problems of polling-station voting can be reduced by having a booth containing a public access computer dedicated to remote electronic voting, so that people who bring their voting credentials with them can vote on it.

261. It is likely that the most secure way of dealing with multiple electronic votes is to accept only the first electronic vote received (the alternative is accepting the last, which would open up new attack possibilities.)

262. The priority of physical versus electronic ballots is more difficult, and it is not intended to fully answer the question here as there are arguments in both directions.

C.5 Vote Counting

263. Up to this point we have glossed over exactly how it is proposed that ballots are counted. Ballot counting is an important part of the election process, as for example a single large database that performs all of the functions of counting would rightly be considered a single point of weakness.

264. This proposal therefore uses a more distributed architecture and is illustrated below.

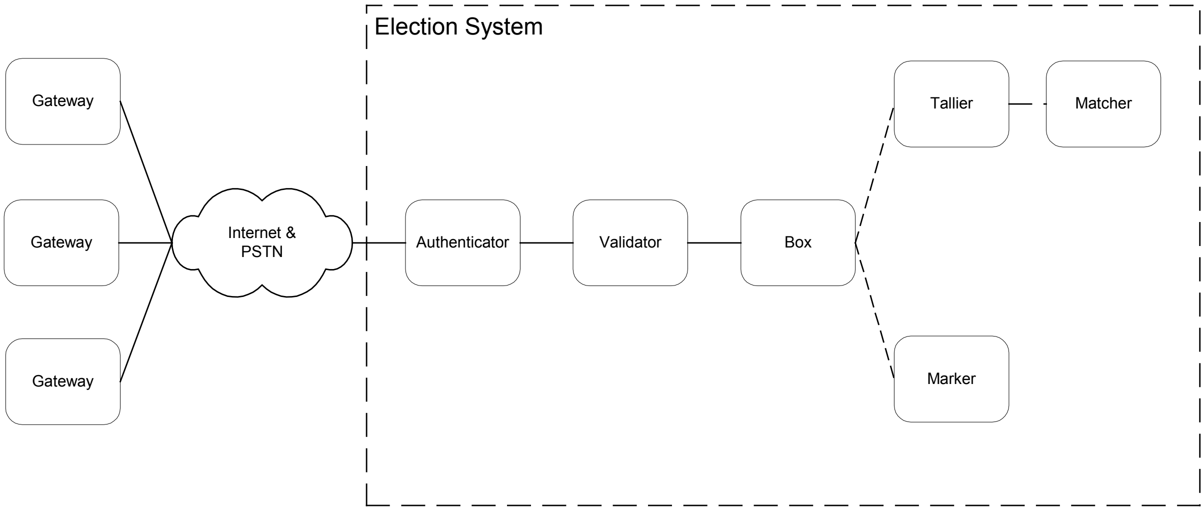

Figure 4: Detailed Voting Architecture

265. We now discuss the components in more detail. The first system that votes enter will be the Gateway.

C.5.1 Gateway

266. As Remote Electronic Voting will potentially use a number of different delivery channels, each will need its own gateway systems. In the case of Internet voting these will be web servers, and similarly there will be computers handling SMS communications, touch-tone telephone and so forth.

267. These systems will be under the control of the election authority, so they will - to a point - be trusted. Gateways will be configured to sign and then encrypt votes passing through them. Applying a digital signature also allows other elements of the system to keep track of where a vote was cast. Votes without valid signatures will not be counted in the final reckoning.

268. Gateways will keep an audit log of all votes sent to them. Note that at this stage no checking has been performed as to the validity of the vote. This function is not carried out by the gateway, so when logged, signed, and encrypted a vote will be passed on to a system known as the Authenticator.

C.5.2 Authenticator

269. The Authenticator is responsible for checking the Voter ID in the message. After decrypting the vote received from the gateway, the Authenticator will look up the submitted Voter ID on its list of valid Voter IDs. If the Voter ID is invalid then a message along the lines of:

```
Invalid Vote. Remember to vote carefully.
```

will be sent back to the voter via the Gateway.

270. If the Voter ID is valid then the secret function corresponding to the Voter ID will be used to generate a Response ID based on the submitted PCIN. This will **not** be returned to the voter at this stage.

271. The Voter ID and generated Response ID will then be submitted to the Validator.

C.5.3 Validator

272. The Validator stores only a list of Voter IDs and the corresponding valid Response IDs. If it receives a valid pair of IDs from the Authenticator, it will permit the vote held by the Authenticator, and the corresponding Response ID, to be passed to the system known as the Box.

C.5.4 Box

273. By the time a vote reaches the Box we know that it contains a valid Voter ID, and implicitly that its PCIN is valid (as a valid Response ID was generated from it). This system represents the traditional ballot box and will store the votes until the close of polls.

274. At the close of polls, the Tallier is brought on line and the contents of the Box are passed to it.

C.5.5 Tallier

275. The Tallier holds a list of Voter IDs, PCINs, constituency numbers and candidate numbers. Before tallying each vote, the digital signature on a vote is checked, and if the signature is correct the candidate in the constituency corresponding to the Voter ID and PCIN will be awarded a vote. Note that the Tallier does not know the identity of the candidates and constituencies.

276. It is possible that several Talliers in parallel will count the votes in this way. The totals of votes will be passed on to a system called the Matcher.

C.5.6 Matcher

277. The Matcher has a simple rôle, which is to de-anonymise the constituency/candidate numbers in order to produce a result of the electronic part of the election. These can then be added to any paper totals in order to give the complete, final result.

C.5.7 Marker

278. In addition, if required, a separate system - the Marker - can use the Voter IDs extracted from the votes held in the Box in order to produce marked copies of the electoral roll showing who voted electronically.

C.5.8 A Note on Counting

279. The above description of counting systems is illustrative of the envisioned system, but obviously care must be taken in the implementation of the system to

ensure that no one system is in a position to undetectably discard votes, etc., and that no one person is in a position to control enough of the disparate system to alter the tallies of votes.

280. For example, the back-end of the counting architecture will employ comprehensive logging and appropriate cryptographic techniques to make it impossible for single systems to undetectably remove or insert votes.

C.6 Summary

281. In conclusion we have presented a system for practical remote electronic voting that supports multiple voting channels whilst placing no demands on the client systems.

Annex D. References

[1] Office of the e-Envoy, In the service of democracy: a consultation paper on a policy for electronic democracy, July 2002, http://www.edemocracy.gov.uk

[2] Dr. Lawrence Pratchett, *et al*, The Implementation of Electronic Voting, May 2002, http://www.dmu.ac.uk.

[3] Office of the e-Envoy, E-government strategy framework policy and guidelines: Security, Version 2.0, 02 November 2001, http://www.e-envoy.gov.uk.

[4] Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta. “A practical secret voting scheme for large scale elections”. In Jennifer Seberry and Yuliang Zheng, editors, *Advances in Cryptography--AUSCRYPT '92*, volume 718 of *Lecture Notes in Computer Science*, pages 244-251, Gold Coast, Queensland, Austrailia, 13-16 December 1992, Springer-Verlag.

[5] Lorrie Faith Cranor and Ron K. Cytron, “Sensus: A Security-Conscious Electronic Polling System for the Internet”, *Proceedings of the Hawaii International Conference on System Sciences* , January 7-10, 1997, Wailea, Hawaii, USA.

[6] Mark A. Herschberg, *Secure Electronic Voting Using the World Wide Web*, Master's Thesis, Massachusetts Institute of Technology, June 1997.

[7] Lorrie Faith Cranor, “Electronic Voting - Computerized polls may save money, protect privacy”, *ACM Crossroads Student Magazine*, 24 April 1996.

[8] Statement on Electronic Voting, http://mainline.brynmawr.edu/~rmercuri/, 2001, Rebecca Mercuri.

[9] Rebecca Mercuri , *Electronic Vote tabulation: checks & balances*, Phd Thesis, University of Pennsylvania, 2001.

[10] Peter Neumann, “Notes on a Hearing for California Assembly Committee Election Reapportionment and Constitutional Amendments”, January 2001.

[11] Peter Neumann, “Security Criteria for Electronic Voting”, SRI International, presented at 16th National Computer Security Conference Baltimore, Maryland, September 1993.

[12] Bruce Schneier, Crypto-gram Newsletter, December 2000.

[13] Ronald Rivest, Statement to CalTech-MIT VTP Press Conference, 16th July 2001.

[14] Ronald Rivest, Testimony to Committee on House Administration, 24th May 2001.

[15] Caltech-MIT Voting Technology Project, “Voting - What is, What Could Be”, July 2001,

[16] California Internet Voting Taskforce, “A Report on the Feasibility of Internet Voting”, January 2000.

[17] US Department of Defense, DoD Washington Headquarters Services Federal Voting Assistance Program: Voting Over the Internet Pilot Project Assessment Report, June 2001.