941 # Appendix A: Internet Voting Security Concerns

Concerns raised on Internet voting		Resulting Technical Threats	Possible generic security service countermeasure
1.	Impersonation of the right to vote. The concern here is that a person attempts to impersonate to be a legitimate voter when he/she is not. The initial task of verifying that a person has the right to vote must be part of the voter registration process. A person must not be given the right to vote until after proper due diligence has been undertaken during voter registration that the person has a right to vote in a contest.	Inadequate, incorrect or improper identification of person during registration of voters	Trusted voter identification and registration using: Security Procedures. Best Practices. Secure communications channels. The voter registration authority must follow standard Security Operating Procedures (SOPs) which ensure due diligence has been done.
		Inadequate privacy of the exchange between the person and the electoral system during voter registration	Channel between voter and registration system must provide: Connection Confidentiality Connection Integrity
2	Voter is not presented with correct ballot information due to incorrect candidate identification.	Incorrect identification during candidate registration.	Trusted candidate identification and registration are needed using: - Security Procedures. - Best Practices. - Secure communications channels. - Authentication and identification of candidates The candidate registration must follow standard Security Operating Procedures (SOPs) which ensure due diligence has been done.
3	Registration system impersonation	Inadequate authentication of registration system	Channels to and from the registration system must provide point to point authentication.

4	Impersonation of a legitimate registered voter	Incorrect authentication at the time of casting vote.	Trusted voter authentication (i.e. the right to cast a vote in this contest)
		Inadequate privacy of the exchange between the voter and the electoral system when vote is cast.	Channel to provide: - Connection Confidentiality - Connection Integrity - Between voter and e-voting system
5	Obtaining the right to vote illegally from a legitimate voter. This may be by intimidation, theft or by any other means by which voting right has been obtained illegally. For example, by Stealing a voting card from a legitimate voter.	Stealing the voter's voting card (e.g. the VToken data).	Some secret data only known to the voter's is required to be presented at the time of casting a vote. Before a vote is counted as a valid vote proof must be provided that the voter's secret data was present at the time of casting the vote.
		Any means of getting a legitimate voter to reveal his VToken data.	
6	Voting system impersonation	Inadequate authentication of registration system	Channel to provide: Point to point authentication
		Inadequate authentication of voting casting point (e.g. polling station/ballot box)	Channel to provide: Point to point authentication
7	Voter is not presented with correct ballot information	Inadequate integrity of the ballot information Given to the user Held in the voting system	Trusted path to voter on ballot options
			Integrity of the ballot information
			Integrity of cast votes
		The casting options available to the voter are not genuine	Trusted path between voter and vote recording
		Trojan horse, man in the middle attack	Trusted path to voter on ballot options
8	How do I know the voting system records votes properly	Integrity of the voting system	Non-repudiation of the vote
			Non-repudiation the vote was cast by a genuine voter
			Audit of voting system
			Connection confidentiality
		Insecure channel between the voter and the vote casting point	Connection Integrity
			Connection Confidently

		Voter's intent is recorded accurately	Trusted path between voter and vote recording
			Non-repudiation of the vote recorded
		Proof that a genuine vote has been accurately counted	Audit
9	How can I be sure the voting system will not disclose whom I have voted for	Voter's identification is revealed	Voter's identification is anonymous
			Vote confidentiality
10	How can it be sure that my vote has been recorded	Loss of vote	Proof of vote submission
11	How can I be sure there is no man-in-the- middle that can alter my ballot	Vulnerable client environment; Trojan horses Virus	Physical security
			Procedural security
			Unpredictable Coded voting information
		Interception of communication	Integrity of communications channel between client and server system
12	All votes counted must be have been cast by a legitimate voter	Voter impersonation	Voter authentication
		Audit facility fails to provide adequate proof	Non-repudiation of the vote record
			Non-repudiation that legitimate voters have cast all votes.
		Breaking the vote counting mechanisms	Independent audit
13	Only one vote is allowed per voter, per contest	Voter impersonation at registration	User registration security Procedures Voter Identification
		Multiple registration applications	
		Multiple allocation of voters credentials	Voter authentication
14	The vote cannot be altered from the voter's intention	Vulnerable client environment; Trojan horses Virus	Trusted path from voter's intent to vote record
			Vote integrity
			Vote non-repudiation
15	The vote may not be observed until the proper time	Votes may be observed before the end of the contest	Voter confidentiality
16	The voting system must be accountable and auditable		Non-repudiation of vote data.
			Audit tools

17	Identification and authentication information to and from the voter must be privacy protected	Loss of privacy	Channel to provide: Connection Confidentiality
18	The voter's actual identity may need to be anonymous	Voter's identification is revealed Denial of service attack	Voter's identification is anonymous
19	Denied access to electronic voting station		This needs to be counted by engineering the system to provide survivability when under denial of service attack.