Federal Voting Assistance Program
Comparative Risk Analysis of the Current UOCAVA Voting System and an Electronic Alternative Report
Vulnerability-Threat Database (VTDb)

Index ID	Source ID	Threat Vector	Threat Event	Vulnerability	Threat Agent Category	Threat Agent(s)	Potential Mitigation	Source	Reference
1	1A-1	Out of date registration	A voter moves and forgets to inform the election official of his/her new address.	Human error: there are no mechanisms to warn voters that their data is out of date.	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
2	1A-2	No access to form or instructions	Voter unable to obtain form and instructions.	Voters may not know how to locate his or her voting assistance officer or have access to the fvap's voting assistance guide or website	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
3	1A-3	Unclear form or instructions	Voter unable to understand form or instructions.	Voter registration applications and/instructions may be unclear.	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
4	1A-4	Illegible handwriting	Voter's handwriting is illegible such that the voter cannot be registered.	Registration forms may be marked by hand.	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
5	1A-5	Registration form incomplete	Voter does not complete form (e.g., required information missing).	Registration forms may be marked by hand, which lacks error-checking mechanisms.	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
6	1A-6	Mistakes on registration form	A voter provides incorrect information.	Out-of-date election resources, human error	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
7	1A-7	Unable to locate help	Voter is unable to find help.	Information about help is not always widely available or easy to find.	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
8	1A-8	No access to mail service	Voter does not have access to mail service.	Mail services are not available in every location.	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
9	1A-9	Returned to wrong election official	Completed application is sent to wrong location and/or election official.	There are no mechanisms in place to ensure the completed application is sent to the correct address.	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
10	1A-10	Mangled application	Completed application is mangled on receipt by election official.	Equipment used in mail system may mangle mail.	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
11	1A-11	Incorrect or insufficient postage	The application is mailed back with incorrect or lack of postage.	There are no checks in place to ensure proper postage.	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
12	1A-12	Registration form delivery failure	Voter registration application is lost or significantly delayed en route to the election official.	Foreign and domestic mail services are not fully reliable.	human-unintentional	mail employee; ISP technician	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
13	1A-13	Fake registration form	A voter is provided a fakee registration form and instructions.	There are no mechanisms to ensure a voter obtains the correct registration form.	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
14	1A-14	Voter obtains incorrect form	A voter obtains the incorrect form and or instructions.	Out-of-date election resources, human error	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
15	1A-15	Voter prevented from registering	Voter is prevented from completing the registration form.	Lack of supervised or controlled environment	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
16	1A-16	Registering ineligible voters	An individual attempts to register ineligible voters (e.g, voters from nearby jurisdictions, non-citizens, dead voters)	There are no mechanisms ensuring a voter can only attempt to register themselves	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
17	1A-17	False assistance provided to voters	An election official intentionally provides incorrect assistance to a voter	Election official may know voter's party affiliation and want to prevent certain parties from voting.	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
18	1A-18	Failure to mail registration form	Voter forgets to send registration form to election official.	Human error	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
19	1A-19	Flood of ballots	An individual floods the election official with false registration applications.	Human processing is necessary to proof registration applications.	human-deliberate	malicious outsider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
20	2A-1	Ineligible voter registered	An ineligible voter is registered to vote.	Weak identity proofing mechanisms in the registration process.	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
21	2A-2	Eligible voter not registered	An eligible voter is denied voter registration.	Weak identity proofing mechanisms in the registration process.	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
22	2A-3	Vrdb not updated	Application from unregistered voter is not added or saved to vrdb.	Limited automated error checking during application processing.	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
23	2A-4	Wrong record in vrdb selected	Wrong record is selected for updating/merging.	Limited automated error checking during application processing.	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
24	2A-5	Data entry error	A mistake is made when copying the data from the application into the vrdb record for the voter.	Limited automated error checking during application processing.	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
25	2A-6	Uocava voter improperly flagged	A uocava voter is not flagged in vrdb as a uocava voter.	Uocava voters are not automatically flagged, software error	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
26	2A-7	Failure of state verification systems	State verification systems fail (e.g., process of verifying driver's license numbers does not work).	Reliance on driver's license and ssa databases to verify numbers.	equipment failure	hardware; software	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
27	2A-8	Registration form not received	Election official does not receive voter registration form	Foreign and domestic mail services are not fully reliable.	human-unintentional	mail employee; ISP technician	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
28	2A-9	Intentional loss of registration form	Election official intentionally loses voter registration form	Insufficient checks and balances on privileged election process	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
29	2A-10	Destruction of registration forms	Hostile individual/group spoils, destroys or manipulates registration forms or registration processes	Poor physical security mechanisms, insufficient checks and balances on privileged election process	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
30	2A-11	Vrdb crash	Vrdb is corrupted or crashes	Substantive software errors or software configuration error	equipment failure	hardware; software	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
31	2A-12	Malicious code within vrdb	Vrdb performs different actions for certain classes of voters	Software contains malicious code	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
32	2A-13	Official refusing to register voter	Election official intentionally does not enter voter into vrdb	Insufficient checks and balances on privileged election process	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
33	2A-14	Official not verifying eligibility	Election official intentionally does not verify voter eligibility	Insufficient checks and balances on privileged election process	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
34	2A-15	Accidental voter registered	Election official does not follow the legally mandated procedures for qualifying voters	Changing or confusing qualification requirements	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
35	2A-16	Failure to send denial of registration	Election official does not send denial of registration to voter	Human error	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
36	2A-17	Intentionally not sending denial of registration	Election official intentionally does not send denial of registration to voter	Insufficient checks and balances on privileged election process	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
37	2A-18	Voter unaware of denial of registration	Voter never receives denial of registration	Foreign and domestic mail services are not fully reliable.	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
38	2A-19	Ineligible voter records in vrdb	Ineligible voters not removed from the list of registered voters	It is often difficult for states to compare voter registration databases between states and to match the voter rolls with death records.	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
39	3A-1	Election official misaddresses ballot	A ballot packet is misaddressed by the election official during ballot packet creation (e.g., incorrect use of abbreviations).	Ballot packet addressing may be a manual or semi-automated process.	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
40	3A-2	Misaddressed ballot by system	A ballot packet is misaddressed during ballot packet creation due to a bug in the absentee voter management software (e.g., complete address is cut off).	Error in voting system software.	equipment failure	hardware; software	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013

Index ID	Source ID	Threat Vector	Threat Event	Vulnerability	Threat Agent Category	Threat Agent(s)	Potential Mitigation	Source	Reference
41	3A-3	Delays in printing ballots	Litigation delays printing of ballots	Timeline for judicial challenges often backs into deadlines for printing ballots.	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
42	3A-4	Printing errors	There are errors in the printed ballots (e.g., mistakes on ballots, printer sending the wrong ballots, etc.).	Reliance on third-party ballot printers	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
43	3A-5	Changes to final ballot	There are changes to the candidates on the final ballot.	Judicial challenges could result in candidate deemed ineligible or candidate dies.	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
44	3A-6	Wrong ballot sent to voter	Wrong ballot or materials are sent to voter.	Ballot packet processing may be a manual or semi-automated process.	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
45	3A-7	Delay or mistake in non-ballot materials	Printing delay or mistake in collateral balloting materials (e.g., return envelope with oath, instructions).	Printer makes mistake or is delayed printing collateral balloting materials.	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
46	3A-8	Last minute change	Last minute change to absentee voting materials and procedures (e.g., late change to law).	Lawmaking body or court changes rules for absentee voting.	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
47	3A-9	Lost or delayed delivery	A blank ballot is lost or delayed by a mail service en route to the voter.	Mail delivery systems are not fully reliable.	human-unintentional	mail employee; ISP technician	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
48	3A-10	Omission of materials	Omission of information in packet—either ballot or collateral materials	Human error	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
49	3A-11	Intentional omission of materials	Ballot materials are intentionally incorrect or omitted from ballot packet	Insufficient checks and balances on privileged election process	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
50	3A-12	Ballot production software malfunction	Ballot production software malfunctions, impacts timeframe	Election officials may have a single copy of the ballot production software installed on a single computer	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
51	3A-13	Incorrect voter list	Election official accidently generates an incorrect uocava voter list	Substantive software errors or software configuration error	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
52	3A-14	Intentionally incorrect voter list	Election official intentionally generates an incorrect uocava voter list	Insufficient checks and balances on privileged election process	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
53	3B-5	Scanned ballot is unreadable	Scanned ballot is unreadable	Election official scanner does not produce a readable attachment	equipment failure	hardware; software	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
54	3B-6	Malfunctioning scanning device	Election official scanner broken	Cannot create ballot for email	equipment failure	hardware; software	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
55	3B-7	Cannot transfer ballot	Ballot image will not transfer from scanner to the election official's computer	Software configuration problem	equipment failure	hardware; software	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
56	3B-8	Ballot tampering before sending	Ballots tampered with prior to sending	Election official computer system	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
57	3B-9	List of voter emails deleted	Email list of voters is deleted	Insufficient integrity protections or access control mechanisms on e-mail list	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
58	3B-10	Error in mail merge	When doing automatic mail merge, documents won't attach to email	Data files or software has a bug that prevents attachment causing the need for a manual process for large amounts of ballot requests	equipment failure	hardware; software	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
59	3B-11	Incorrect ballot attached to email	Person attaches wrong ballot or materials to email	Human error	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
60	3B-12	Intercepting & tampering email	Email intercepted and tampered with after sending	Email is unprotected	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
61	3B-13	Intercepting & blocking email	Attacker intercepts and blocks email	Email is unprotected	human-deliberate	malicious outsider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
62	3B-14	Email blocked – improper configuration	Outgoing e-mails are blocked due to improper server configuration.	Improper server configuration (e.g., attachment limits too small)	equipment failure	hardware; software	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
63	3B-15	Delays in creating ballot definitions	Delay in creating digital ballots or collateral material	Software error	equipment failure	hardware; software	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
64	3B-16	Accidental package of malware	Election official accidentally packages malware (e.g., tracking mechanisms, scareware) into ballots or collateral materials	Human error, computer security procedures	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
65	3B-17	Intentional malware injection	Election official intentionally injects malware (e.g., tracking mechanisms, scareware) into ballots or collateral materials	Insufficient checks and balances on privileged election process	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
66	3B-18	Incompatible ballot filetype	Election official creates ballot in incompatible format (e.g., filetype, papersize)	Human error	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
67	3B-19	Incorrect vrdb export	Vrdb does not properly export some or all flagged uocava voters and/or associated voter information (e.g., email address, ballot style)	Software error	equipment failure	hardware; software	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
68	3B-20	Loss of or leaked list of voter email	Election official loses or leaks list of voter emails	Human error, computer security procedures	human-deliberate; human-unintentional	malicious insider(s); local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
69	3B-21	Isp blocks election office	Isp blocks election official believing they are running a spamming operation.	False positive in network monitoring of isp	equipment failure	hardware; software	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
70	3B-22	Attacks on Internet infrastructure	Hostile group attacks or degrades dns servers - prevents emails from reaching voters	Mx records are necessary for emails to traverse the Internet	human-deliberate	malicious outsider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
71	3C-2	Errors in generated ballots	There are errors in the generated ballots or ballot definition files.	Human error or error in the ballot creator software.	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
72	3C-3	Logic errors in generated ballots	There are logic errors in the generated ballots/ballot definitions (e.g., timing marks are incorrect, n-of-m voting is incorrect).	Human error or error in the ballot creator software.	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
73	3C-6	Incorrect ballots placed on webserver	The wrong ballots are loaded onto the webserver	Failure to provide all information.	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
74	3C-7	Server provides incorrect configured ballot	The web server/application provides the incorrect ballot style to the voter.	Human error or an error in the voting system software.	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
75	3C-8	Incorrect account configuration	Voter accounts are not configured properly on the web server, so that voters do not receive the proper ballot style.	Human error or an error in the voting system software.	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
76	3C-9	Incorrect password/pin configuration	Passwords/pins are not configured properly in the voting system.	Human error or an error in the voting system software.	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
77	3C-10	Password/pin leakage	An attacker learns the passwords/pins for voters.	Passwords/pins could be generated improperly or insecurely; or, passwords/pins are not properly protected on the voting system.	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
78	3C-11	Passwords/pins stolen	Passwords/pins are stolen by an insider when they are generated or distributed to voters.	Passwords/pins are generated in plaintext and must be distributed to voters in plaintext.	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
79	3C-12	Passwords/pins interception	An attacker intercepts passwords/pins en route.	Passwords/pins are transmitted to voters in plaintext (typically by mail or email)	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
80	3C-13	Delayed password/pin	The password/pin is delayed or disrupted in transit to the voter.	Unreliable mail service, delays associated with mail forwarding, or disruptions in e-mail servers.	equipment failure	hardware; software	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
81	3C-14	Attacker modifies voting system	An attacker gains unauthorized access to webserver and modifies critical voting materials or software.	Insecure server configuration or vulnerabilities in the voting system software.	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
82	3C-15	Delay in creating ballots/materials	Delay in creating digital ballots or collateral materials	Software error	equipment failure	hardware; software	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
83	3C-17	Malware intentionally sent to voter	Election official intentionally packages malware (e.g., tracking mechanisms, scareware) into ballots or collateral materials	Insufficient checks and balances on privileged election process	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
84	3C-18	Generating weak passwords	Election software generates weak passwords and stores them insecurely	Security design flaw	equipment failure	hardware; software	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
85	3C-19	3rd party access to webserver	Election official or other inside party provides access to webserver or web application	Insufficient checks and balances on privileged election process	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
86	3C-20	Wrong password sent to voter	Wrong password is sent to voter	Email client or ballot printer depending on distribution mechanism	equipment failure	hardware; software	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
87	3C-21	Error in pin/password packets	Election worker improperly creates pin/password packets	Pin/password may be lost	equipment failure	hardware; software	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
88	3C-22	3rd party intercepts ballots	Hostile individual/group intercepts ballots during insecure upload (e.g, via the Internet, plaintext)	Lack of confidentiality and integrity mechanisms in upload process	human-deliberate	malicious outsider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013

Index ID	Source ID	Threat Vector	Threat Event	Vulnerability	Threat Agent Category	Threat Agent(s)	Potential Mitigation	Source	Reference
89	3C-23	Webserver infected with malware	Hostile individual/group places malware on election webserver	Webservers are openly exposed to the Internet.	human-deliberate	malicious outsider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
90	3C-24	Denial of service to webserver	Hostile group ddoss election webserver	Webservers are openly exposed to the Internet.	human-deliberate	malicious outsider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
91	4A-1	Lost or delayed ballot in mail	A marked ballot is lost or delayed by a mail service en route to a election official.	Foreign and domestic mail services are not fully reliable.	human-unintentional	mail employee; ISP technician	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
92	4A-2	Error when marking ballot	The voter spoils the ballot by making an accidental error when marking the ballot.	Human error, inability to correct mistakes on ballot	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
93	4A-3	Voter forgets to sign affidavit	The voter forgets to sign the affidavit, which is required for absentee voters.	Affidavits must be hand-signed, which lacks error-checking mechanisms.	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
94	4A-4	Ballot or required forms not in envelope	Ballot or other required forms are not inserted into return envelope.	Human error	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
95	4A-5	Return envelope not sealed	Return envelope is not sealed.	Human error	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
96	4A-6		The voter receives the wrong ballot style.	Human error	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
97	4A-7	Ballot not mailed prior to deadline	The voter forgets to mail the ballot prior to the deadline.	Human error	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
98	4A-8	Wrong ballot returned	Wrong ballot is returned by voter.	Human error; lack of easily-identifying information on ballots	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
99	4A-9	Undue influence	Undue influence over voter when voting ballot.	Lack of supervised/controlled environment	human-deliberate	malicious outsider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
100	4A-10	Ambiguous marks	The voter makes ambiguous marks on the ballot, which optical scanners and election officials may have difficulty interpreting.	Human error	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
101	4A-11	Incorrect address	Ballot mailed back incorrectly addressed	There are no mechanisms in place to ensure the completed application is sent to the correct address.	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
102	4A-12	Insufficient postage	Incorrect or insufficient postage.	There are no checks in place to ensure proper postage.	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
103	4A-13	Delivery failure to election official	Ballot delivery failure to election official	Voter may not know there was issue with ballot return	human-unintentional	mail employee; ISP technician	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
104	4A-14	Retrieved by wrong party	Ballot retrieved by someone other than intended voter	Ballot packets are not stored in a secure manner after mail delivery.	human-deliberate	malicious outsider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
105	4A-15	Mail prevented from reaching voters	Mail system employee intentionally prevents mail from reaching voters	Insufficient checks and balances in mail system	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
106	4A-16	Mail delivered to incorrect location	Ballots are delivered to incorrect location	Foreign and domestic mail services are not fully reliable.	human-unintentional	mail employee; ISP technician	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
107	4A-17	Military base cannot receive ballots	Military base does not have location to receive ballots packets	Active combat zones may not receive mail	human-unintentional	mail employee; ISP technician	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
108	4A-18	Mail employee destroys ballots	Mail employee intentionally destroys or spoils ballot packets	Insufficient checks and balances in mail system	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
109	4A-19	Ballots lost in mailroom	Mail lost in mailroom	Foreign and domestic mail services are not fully reliable.	human-unintentional	mail employee; ISP technician	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
110	4A-20	Incapacitated voter cannot retrieve ballot	Voter injured or incapacitated and cannot retrieve ballot packet	Military voters may reside within active warzones	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
111	4A-21	Mark ballot in an attempt to sell	The voter makes personally identifying marks in an attempt to sell their vote	It is difficult to determine if a voter has encoded a selection pattern into a ballot	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
112	4A-22	Voter returns fake ballot	The voter intentionally marks and returns a fake ballot	Ballot authentication mechanisms	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
113	4A-23	Malicious object sent to election office	The voter sends a malicious object back to the election office	Malicious object detection processes of mail system	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
114	4A-24	3rd party removes affidavit	3rd party removes either affidavit or ballot from returned materials	Ballot packets are not stored in a secure manner before being sent to election official	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
115	4A-25	Use of materials from previous election	The voter uses materials (e.g., ballot, envelope) from previous election	Older election materials may look similar to current election material	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
116	4B-1	Unknown username/password	Voter doesn't know log-in username and password	Human error	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
117	4B-2	Voter cannot login	Voter cannot log in because email client is down	Email systems are unreliable	equipment failure	hardware; software	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
118	4B-3	Voter logs into fake website	Voter logs into fake website	People are susceptible to phishing attacks	human-deliberate	malicious outsider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
119	4B-4	Denial of service on e-mail system	Denial of server attack on e-mail system	Inoperable email system or because database altered maliciously	human-deliberate	malicious outsider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
120	4B-6	Ems misaddresses ballot	A ballot packet is misaddressed by the election official during email creation	Ballot packet addressing may be a manual or semi-automated process.	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
121	4B-7	Wrong ballot retrieved by voter	Wrong ballot type is retrieved by voter via malicious attack	Server compromised	human-deliberate	malicious outsider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
122	4B-8	3rd party retrieves and deletes ballot	3rd party retrieves ballot for voter and deletes ballot	Multiple individuals may share the same e-mail address.	human-deliberate	malicious outsider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
123	4B-9	Voter deletes email containing ballot	Voter accidently deletes email containing ballot	Human error	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
124	4B-10	Voter unable to open attachment	Voter unable to open attachments	Lacking required software (i.e. adobe)	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
125	4B-11	Voter unable to print ballot	Voter cannot print ballot	Voter does not have printer or printer does not have adequate supplies (e.g. ink, toner, paper)	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
126	4B-12	Problem in ballot printing	Ballot cannot be printed or prints incorrectly	Election officials may not optimize ballots for printing in countries with alternative printing sizes and configurations	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
127	4B-13	Spam filter marks ballot as spam	Spam filter marks email as spam	Use of third-party bulk e-mailer.	equipment failure	hardware; software	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
128	4B-14	Voter's system infected with malware	Voter's system infected with malware	Common document formats can contain malware	equipment failure	hardware; software	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
129	4B-15	Transmission failure due to attachment size	Emailed ballot not delivered to voter because attachment to large.	Some email systems cannot deliver emails over a certain size threshold.	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
130	4B-16	Voter selections sent to 3rd party	Onscreen marking captures and transmits a voter's ballot selections to a hostile/individual group.	Voter's cpu	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
131	4B-17	Digital ballot not accessible	Voter cannot mark choices because ballot is not compatible with personal assistive technology	Ballot format/voter's technology	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
132	4B-18	Ambiguous marks on ballot	The voter makes ambiguous marks on the ballot which optical scanners and election officials may have difficulty interpreting.	Human error	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
133	4B-19	Undue influence	Undue influence over voter when marking ballot.	Lack of supervised/controlled environment	human-deliberate	malicious outsider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
134	4B-20	Information not inserted into envelope	Ballot or other required forms are not inserted into return envelope.	Human error	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
135	4B-26	Software modifies voter choices	When onscreen marking is used malicious software modifies voter's choices before printing	Common document formats can contain malware	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
136	4C-1	Voter cannot locate election website	Voter does not know where to find the election web site.	Insufficient communication with voters.	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
137	4C-2	Voter unable to use election website	The voter is unable to use the web site.	Confusing design, lack of accommodations for voters with disabilities.	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
138	4C-3	Voter is unable to print ballot/materials	The voter is unable to print the ballot and associated materials.	Voter does not have printer or printer does not have adequate supplies (e.g. ink, toner, paper)	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
139	4C-14	Denial of service on website	Web site is not accessible due to a denial of service attack.	Web site is publicly accessible on the Internet.	human-deliberate	malicious outsider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
140	4C-15	Individuals impersonating voters	A malicious individual obtains voters' credentials and impersonates voters.	Passwords/pins could be generated improperly or insecurely; or, passwords/pins are not properly protected on the voting system.	human-deliberate	malicious outsider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
141	4C-16	Voter receives incorrect ballot style	Voter receives the incorrect ballot style.	Vulnerability in the voting system allows an attacker to modify election/system files.	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
142	4C-17	Voters redirected to malicious website	Voters are redirected to another web site without their knowledge.	Vulnerabilities in voters' computers or network infrastructure components (e.g., dns, routing, etc).	human-deliberate	malicious outsider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
143	4C-18	Voter loses password/pin	Voter loses password/pin prior to the election.	Human error	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013

Index ID	Source ID	Threat Vector	Threat Event	Vulnerability	Threat Agent Category	Threat Agent(s)	Potential Mitigation	Source	Reference
144	4C-19	Voter does not receive login credentials	Voter does not receive login credentials	Credential distribution process may be unreliable (e.g., email, mail system)	equipment failure	hardware; software	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
145	4C-20	Voters credentials are stolen	Voters are phished (logs into false site, credentials are stolen). attackers cast the voter's ballot.	It is difficult to distinguish between extremely similar websites	human-deliberate	malicious outsider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
146	4C-21	Ballot altered during transmission	Ballot altered in transmission to voter	No confidentiality or integrity mechanisms within ballot distribution system	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
147	4C-22	Ballot prints incorrectly	Ballot prints incorrectly (e.g., too small for page)	Election officials may not optimize ballots for printing in countries with alternative printing sizes and configurations	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
148	4D-18	Voting server compromised	Attackers in control of the voting server learn how a large group of voters cast their ballots.	Vulnerabilities in the voting system server.	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
149	4D-19	Malware modify ballot before printing	Malware on a voters' machines modifies voters' ballots prior to printing.	Insecure computers owned and operated by voters.	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
150	4D-20	Voting server controlled by 3rd party	Attackers in control of the voting server attempt to modify voters' ballots prior to printing.	Vulnerabilities in the voting system server.	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
151	4D-22	Voters credentials are stolen	Voters are phished (logs into false site, credentials are stolen)		human-deliberate	malicious outsider(s)		NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
152	4D-23	3rd party sniffs traffic to breach privacy	Attackers sniff traffic while voters are casting ballots to learn how they voted	No confidentiality or integrity mechanisms on votes in transit to webserver or logic to keep voter's selections on their pc	human-deliberate	malicious outsider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
153	4D-25	App engineered to breach privacy	Malicious election official/programmer engineers web application to violate voter privacy	Insufficient checks and balances on privileged election process	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
154	4D-26	Unused credentials provided to 3rd party	Election official uses or provides unused login credentials to third party	Insufficient checks and balances on privileged election process	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
155	5A-1	Valid signature rejection	A valid voter signature is rejected.	Human error in signature verification	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
156	5A-2	Invalid signature verification accepted	An invalid voter signature is accepted.	Human error in signature verification	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
157	5A-3	Timely ballot is rejected	A timely ballot is rejected.	Human error in determining timeliness.	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
158	5A-4	Untimely ballot is accepted	An untimely ballot is accepted.	Human error in determining timeliness.	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
159	5A-5	Postmark missing or illegible	Postmark date is not present or not legible.	Foreign mail systems do not always affix postmarks or postmarks are not legible.	human-unintentional	mail employee; ISP technician	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
160	5A-6	Receipt of voted ballot not in vrdb	Voter's record is not updated to reflect that voted ballot has been received.	Election official neglects to update voter's record that voted ballot has been received.	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
161	5A-7	Ballot lost or destroyed	Voted ballot is lost or destroyed at election office.	Failure/loss of chain of custody of ballots.	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
162	5A-8	Lost batch of ballots	A batch of ballots is lost or destroyed at the election office	Failure/loss of chain of custody of ballots.	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
163	5A-9	Ballots modified during processing	Marked ballots are modified or replaced during processing.	Limited integrity protections on marked ballots.	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
164	5A-10	Vrdb manipulation	An attacker manipulates the vrdb to reflect that a voter cast another overriding ballot.	Vulnerabilities/weaknesses in vrdb system.	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
165	5A-11	Accidental loss or spoiled ballot packet	Mail service accidentally loses or spoils a ballot packet	Foreign and domestic mail services are not fully reliable.	human-unintentional	mail employee; ISP technician	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
166	5A-12	Intentional loss or spoiled ballot packet	Mail service intentionally loses or spoils a ballot packet	Insufficient checks and balances in mail system	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
167	5A-13	Destruction of mail storage location	Hostile individual/group destroys election official's mail storage location	Poor physical security mechanisms	human-deliberate	malicious outsider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
168	5A-14	Ballots replaced with unofficial ballots	Hostile individual/group swaps mail in election official's mailbox with alternative ballot packets	Poor physical security mechanisms	human-deliberate	malicious outsider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
169	5A-15	Incorrect affidavit signature accepted	Election official finds incorrect signature on file but considers the signature verified	Poor signature verification processes	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
170	5A-16	Software incorrectly authenticates voter	Signature comparison software incorrectly authenticates a voter	Signature verification threshold	equipment failure	hardware; software	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
171	5A-17	Signature software destroyed	3rd party destroys signature comparison software	Poor physical security processes	human-deliberate	malicious outsider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
172	5A-18	Malicious signature software	Malicious signature comparison software can correlate voters to a political party and provides false positives	Poor physical security processes	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
173	5A-19	Election official challenges every ballot	Election official challenges every ballot	Insufficient checks and balances on privileged election process	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
174	5A-20	Voter history not updated	Voter history is not updated due to software error	Software error	equipment failure	hardware; software	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
175	5A-21	Postmark intentionally not verified	Election official intentionally does not check reception and postmark dates	Insufficient checks and balances on privileged election process	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
176	5A-22	Postmark not verified	Election official accidentally does not check reception and postmark dates	Human error	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
177	6A-1	Error in ballot transcription	A returned ballot is incorrectly transcribed to ballot stock or entered onto a dre.	Human error	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
178	6A-2	Ballots incorrectly counted	Voted ballots are not accurately counted.	Errors or vulnerabilities in the voting system.	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
179	6A-3	Results incorrectly aggregated	Election results are not aggregated correctly.	Errors or vulnerabilities in the ems.	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
180	6A-5	Ballot lost or destroyed	A voted ballot is lost or destroyed at the election office.	Failure of loss of chain of custody of ballots	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
181	6A-6	Malicious canvassing board	Malicious canvasing board accepts ballots it should not	Insufficient checks and balances on privileged election process	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
182	6A-7	Canvassing board false positive	Canvassing board unintentionally accepts ballots it should not	Human error	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
183	6A-8	Canvassing board false negative	Malicious canvasing board rejects ballots it should not	Insufficient checks and balances on privileged election process	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013

Index ID	Source ID	Threat Vector	Threat Event	Vulnerability	Threat Agent Category	Threat Agent(s)	Potential Mitigation	Source	Reference
184	6A-9	Acceptable challenged ballots rejected	Canvassing board unintentionally rejects ballots it should not	Human error	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
185	6A-10	Rejected & accepted ballots mixed	Rejected ballots accidently mixed in with accepted ballots	Human error	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
186	6A-11	Rejected & accepted ballots intentionally mixed	Rejected ballots intentionally mixed in with accepted ballots	Insufficient checks and balances on privileged election process	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
187	6A-12	Ballot accidentally damaged	Election worker tears ballot when removing mail envelope	Human error	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
188	6A-13	Unneeded ballot transcription	Election worker states ballot transcription isn't needed when it is	Insufficient checks and balances on privileged election process	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
189	6A-14	Malicious ballot transcription	Election official or election worker intentionally alter the ballot selections of the original ballot during the transcription process	Insufficient checks and balances on privileged election process	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
190	6A-15	Ballot lost during transcription process	Ballot lost during transcription process	Human error	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
191	6A-16	Incorrect election result	Election management software produces incorrect result	Software error	equipment failure	hardware; software	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
192	6A-17	Intentionally incorrect result	Election software programmed to provide incorrect results	Software contains errors or malicious code	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
193	6A-18	Election software failure	Election management software does not start/activate	Software error	equipment failure	hardware; software	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
194	6A-19	Rejected ballots accidently counted	Election official accidently combines rejected ballots with other election results	Not implementing qa processes	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
195	6A-20	Rejected ballots intentionally counted	Election official intentionally combines rejected ballots with other election results	Insufficient checks and balances on privileged election process	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
196	6A-21	Results altered before reported	Results are altered before election official reports election results	Poor physical and computer security processes	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
197	6A-22	Incorrect result intentionally reported	Election official intentionally reports incorrect results	Insufficient checks and balances on privileged election process	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
198	6A-23	Erroneous central count result	Central count scanner software produces incorrect result	Software error	equipment failure	hardware; software	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
199	7A-1	Mail delayed at mail control activity	Mail is delayed at distribution nodes or mail control activity	Mail may be classified as low priority, or the operational risks are too high. weather may also introduce delays	human-unintentional	mail employee; ISP technician	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
200	7A-2	Member no longer at address	The voter is no longer at the address on the ballot and must be forwarded.	Military voters may not have adequate time to inform election officials of their new address when undergoing relocation.	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
201	7A-3	Ballot not scanned into mail system	Voted ballot is not scanned for tracking - the voter believes the ballot is lost when it was actually received	Human error. voter trusts the tracking mechanisms	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
202	7A-4	Voter not known at delivery address	Mail is properly delivered, but the mail handler does not know the voter.	If the mail handler does not know the recipient, the ballot will be returned to the sender. unlike domestic postal delivery, mail is delivered to a unit, which delivers mail to the voter.	human-unintentional	mail employee; ISP technician	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
203	7A-5	Voter moves without leaving forwarding address	A voter transfers without leaving a forwarding address.	Human error. there is no formal process to ensure a voter leaves a forwarding address.	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
204	7A-6	Ballot has incomplete mailing address	Incomplete mailing address on ballot.	Election officials may be unfamiliar with military mailing addresses. critical portions of the address may be inadvertently omitted.	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
205	7A-7	Ballot delayed in postal system not mailed with sufficient time	Ballots not mailed 45 days prior to the election	Mail delivery systems are not completely reliable	human-unintentional	local election official	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
206	7A-8	Mail handler disregards specific ballots	Mail handler deliberately discards or delays ballots from or to a targeted group or jurisdiction.	Ballots do not remain under tight control. insufficient checks and balances on privileged mail process	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
207	7A-9	Mail handler disregards random ballots	A mail handler deliberately discards or delays random ballots.	Ballots do not remain under tight control. insufficient checks and balances on privileged mail process	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
208	7A-10	Mail lost during mail system handling	Mail is accidently lost during handling and processing.	Human and machine error. mail delivery systems are not completely reliable	human-unintentional	mail employee; ISP technician	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
209	7A-11	Outer envelope of ballot damaged/opened	Outer envelope of voted ballot is damaged	Envelopes can be damaged by mail handing equipment or other outside entities.	equipment failure	hardware; software	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
210	7A-12	Voter unable to retrieve ballot	Voter is unable to pick up delivered mail	Military mail facilities have limited operating hours, which may not be compatible with a military member's assigned duties.	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
211	7A-13	Ballot delivered to wrong address	Ballot is delivered to wrong address	Human error. the mail delivery system is not completely reliable.	human-unintentional	mail employee; ISP technician	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
212	7A-14	Ballot incorrectly returned to sender	Ballot may be returned to sender as undeliverable when the address is actually correct	Human error. the mail delivery system is not completely reliable.	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
213	7A-15	Ballot intentionally misrouted	Mail handler intentionally misdirects a ballot to the wrong address.	Insufficient checks and balances on privileged mail process.	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
214	7A-16	Mail system changes ballots	Mail system intercepts and changes ballots in transit	Insufficient checks and balances on privileged mail process	human-deliberate	malicious insider(s)	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
215	7A-17	Mail not retrieved from all areas	Mail system does not pick-up mail from certain areas (e.g., military bases)	Some military zones may be too hostile for mail carriers	human-unintentional	voter	None provided in reference.	NIST	Draft TGDC Risk Worksheets, 8 Jan. 2013
216	Ti2	Voting equipment threats	Attack on Internet voting system	Voting system: remote access to votingsystem; voter attribution	human-deliberate	malicious insider(s)	(1) Only attestable voting platforms	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Rubin, A. D. (2002). Security considerations for remote electronic voting, Communications of the ACM. 45(12), 39-44. Mote, C. D. Jr. (2000). Report of the national workshop on Internet voting: issues and research agenda. ACM International Conference Proceeding Series, 128, 1 - 59.
217	Ti5	Design the attack	Identify requirements and construct the architecture for the malicious software.	Voting system: access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	human-deliberate	malicious insider(s)	(1) High assurance software	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Jefferson, D. (2004) "The Inherent Security Vulnerabilities with Internet Voting", Retrieved from http://aceproject.org/ace-en/topics/et/eth/eth02/eth02b/eth02b4
218	Ti7	Create undervote	Create software that records a vote in a race with no voter selection.	Voting system: access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	human-deliberate	malicious insider(s)	(1) High assurance software (2) Physical vote record (3) Auditing	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007, Retrieved from http://election.dos.state.fl.us/voting-systems/pdf/SAITreport.pdf
219	Ti8	Alter results	Create software that alters the machine's vote tabulation.	Voting system: access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	human-deliberate	malicious insider(s)	(1) High assurance software (2) Physical vote records (3) Auditing	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007, Retrieved from http://election.dos.state.fl.us/voting-systems/pdf/SAITreport.pdf
220	Ti9	Delete contest/candidate	Create software that deletes contests or candidates from the ballot that is presented to the voter.	Voting system: access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption+m30	human-deliberate	malicious insider(s)	(1) High assurance software (2) Auditing	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007, Retrieved from http://election.dos.state.fl.us/voting-systems/pdf/SAITreport.pdf

Federal Voting Assistance Program

Comparative Risk Analysis of the Current UOCAVA Voting System and an Electronic Alternative Report
Vulnerability-Threat Database (VTDb)

Index ID	Source ID	Threat Vector	Threat Event	Vulnerability	Threat Agent Category	Threat Agent(s)	Potential Mitigation	Source	Reference
221	Ti10	Gain necessary knowledge	To be successful, malicious intruders must acquire information that allows them to effectively implement and exercise a malware attack.	Voting machine, sensitive tech data, tech insiders: access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	human-deliberate	malicious insider(s)	None provided in reference.	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007, Retrieved from http://election.dos.state.fl.us/voting-systems/pdf/SAIreport.pdf
222	Ti11	Test the malware	Attackers must be able to test the software that they will use in a voting system attack. this may require acquisition of proprietary software and/or hardware.	Not modeled: access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	human-deliberate	malicious insider(s)	None provided in reference.	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007, Retrieved from http://election.dos.state.fl.us/voting-systems/pdf/SAIreport.pdf
223	Ti12	Replicate environment	In order to test malware, the attacker must be able to create an software/hardware environment that is consistent with the target environment.	Not modeled: access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	human-deliberate	malicious insider(s)	None provided in reference.	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007, Retrieved from http://election.dos.state.fl.us/voting-systems/pdf/SAIreport.pdf
224	Ti13	Simulate the volume	An essential element of testing is to simulate transaction high, medium, and low volume.	Not modeled: access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	human-deliberate	malicious insider(s)	None provided in reference.	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
225	Ti14	Install the malware	The attacker install malware on the target device in order to execute the software to achieve the desired impact.	Servers, pc, terminal: poor security during election artifacts delivery, insecure voter technology	human-deliberate	malicious insider(s)	(1) High assurance software (2) Equipment chain of custody (3) Equipment two person integrity (4) Dedicated use terminal	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Rubin, Avi (2002) "Security Considerations for Remote Electronic Voting over the Internet", Floram Park, NJ: AT&T Labs – Research, Retrieved from http://avirubin.com/e-voting.security.html
226	Ti15	Removable media	Malware installed from removable media that contracted a virus or other regenerating malware.	Servers, pc, terminal: poor security during election artifacts delivery, insecure voter technology	human-deliberate	malicious insider(s)	(1) High assurance software (2) Equipment/media chain of custody (3) Equipment/media two person integrity (4) Strong media authentication	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007, Retrieved from http://election.dos.state.fl.us/voting-systems/pdf/SAIreport.pdf
227	Ti16	Botnet or systematic virus infection	Coordinated effort to install malware across a network on a large number of voting terminals.	Network: poor network security	human-deliberate	malicious insider(s)	(1) Voting terminal not network connected (2) Voting server not network connected (3) Strong network security	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Jefferson, D., A. D. Rubin, B. Simons, and D. Wagner. (2004). Analyzing Internet voting security.Communications of the ACM, 47(10), 59-64.
228	Ti17	Vendor installed	Malicious software may be installed by a member of the vendor's development team.	Not modeled: out of scope	human-deliberate	malicious insider(s)	(1) High assurance software (2) Software chain of custody (3) Employee background checks (4) Strong legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007, Retrieved from http://election.dos.state.fl.us/voting-systems/pdf/SAIreport.pdf
229	Ti18	During l&a	Malicious software may be installed by a member of the logic and accuracy test team.	Servers, pc, terminal: inability to detect the clever insider's infiltration of the l&a test script	human-deliberate	malicious insider(s)	(1) High assurance software (2) Equipment chain of custody (3) Equipment two person integrity (4) Election official background checks (5) Strong legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007, Retrieved from http://election.dos.state.fl.us/voting-systems/pdf/SAIreport.pdf
230	Ti19	During sleepover	Malicious software installed by a pollworker or elections official that has exclusive control of the terminal after l&a and before the election.	Precinct kiosk: poor security during election artifacts delivery	human-deliberate	malicious insider(s)	(1) High assurance software (2) Strong legal deterrence (3) Locked equipment cages for sleepover	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007, Retrieved from http://election.dos.state.fl.us/voting-systems/pdf/SAIreport.pdf
231	Ti20	Trigger the malware	Cause the installed malware to be executed on the target device.	Servers, pc, terminal: poor security of voting equipment	human-deliberate	malicious insider(s)	(1) Strong physical security of devices (2) Poll worker background checks (3) Strong legal deterrence (4) High assurance software	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007, Retrieved from http://election.dos.state.fl.us/voting-systems/pdf/SAIreport.pdf
232	Ti21	Automatic	Design the code in a way that allows automatic execution.	Servers, pc, terminal: poor security of voting equipment	human-deliberate	malicious insider(s)	None provided in reference.	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007, Retrieved from http://election.dos.state.fl.us/voting-systems/pdf/SAIreport.pdf
233	Ti22	Cryptic knock	Design the code to wait for a specific, external action to trigger its full operation.	Servers, pc, terminal: overcoming the defense against cryptic knocks	human-deliberate	malicious insider(s)	(1) Strong physical security of devices (2) Poll worker background checks (3) Strong legal deterrence (4) High assurance software	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007, Retrieved from http://election.dos.state.fl.us/voting-systems/pdf/SAIreport.pdf
234	Ti23	Timing	Utilize a timing trigger to start malware execution.	Servers, pc, terminal: poor security of voting equipment	human-deliberate	malicious insider(s)	None provided in reference.	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007, Retrieved from http://election.dos.state.fl.us/voting-systems/pdf/SAIreport.pdf
235	Ti24	Network attack	Malicious act targeting the network that supports the voting system.	Servers, pc, terminal, network device: poor network security, poor security configuration by admin	human-deliberate	malicious insider(s)	None provided in reference.	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Rubin, Avi (2002) "Security Considerations for Remote Electronic Voting over the Internet", Floram Park, NJ: AT&T Labs – Research, Retrieved from http://avirubin.com/e-voting.security.html

Index ID	Source ID	Threat Vector	Threat Event	Vulnerability	Threat Agent Category	Threat Agent(s)	Potential Mitigation	Source	Reference
236	Ti25	Denial of service	Attempt to prevent voting system operation.	Servers, pc, terminal, network device: poor network security, poor security configuration by admin	human-deliberate	malicious outsider(s)	(1) Service redundancy (2) Strong network security	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Rubin, Avi (2002) "Security Considerations for Remote Electronic Voting over the Internet", Floram Park, NJ: AT&T Labs – Research, Retrieved from http://avirubin.com/e-voting.security.html NIST Andrew Regenscheid and Nelson Hastings, A Threat Analysis on UOCAVA Voting Systems. NISTIR 7551, December 2008, Retrieved from http://vote.nist.gov/uocava-threatanalysis-final.pdf Mote, C. D. Jr. (2002).Report of the national workshop on Internet voting: issues and research agenda. ACM International Conference Proceeding Series, 129, 1-59.
237	Ti26	Flood voting terminal	Creating a high volume of traffic to prevent legitimate information from flowing to/from the voting terminal..	Servers, pc, terminal, network device: poor network security, poor security configuration by admin	human-deliberate	malicious outsider(s)	(1) Redundancy (2) Strong network security	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Rubin, Avi (2002) "Security Considerations for Remote Electronic Voting over the Internet", Floram Park, NJ: AT&T Labs – Research, Retrieved from http://avirubin.com/e-voting.security.html
238	Ti27	Flood voting server	Creating a high volume of traffic to prevent legitimate information from flowing to/from the voting server..	Servers, pc, terminal, network device: poor network security, poor security configuration by admin	human-deliberate	malicious outsider(s)	(1) Redundancy (2) Strong network security	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Rubin, Avi (2002) "Security Considerations for Remote Electronic Voting over the Internet", Floram Park, NJ: AT&T Labs – Research, Retrieved from http://avirubin.com/e-voting.security.html
239	Ti28	Flood supporting network	Creating a high volume of traffic to prevent legitimate information from flowing across the supporting network.	Servers, pc, terminal, network device: poor network security, poor security configuration by admin	human-deliberate	malicious outsider(s)	(1) Strong network security	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Rubin, Avi (2002) "Security Considerations for Remote Electronic Voting over the Internet", Floram Park, NJ: AT&T Labs – Research, Retrieved from http://avirubin.com/e-voting.security.html
240	Ti29	Disable voting component	Destroy or otherwise disable a critical voting system component to stop or slow voting in targeted areas.	Servers, pc, terminal, network device: poor network security, poor security configuration by admin	human-deliberate	malicious outsider(s)	(1) Strong physical security	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Rubin, Avi (2002) "Security Considerations for Remote Electronic Voting over the Internet", Floram Park, NJ: AT&T Labs – Research, Retrieved from http://avirubin.com/e-voting.security.html
241	Ti32	Compromise network device	Attacker exploits a vulnerability that allows her to control or alter communication on a network device.	Network device: poor network security, poor security configuration by admin	human-deliberate	malicious insider(s)	(1) Strong network security	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Rubin, Avi (2002) "Security Considerations for Remote Electronic Voting over the Internet", Floram Park, NJ: AT&T Labs – Research, Retrieved from http://avirubin.com/e-voting.security.html
242	Ti33	Intercept voter transaction	Attack on a network device allows attacker to intercept traffic during a voting session.	Network device: poor network security, poor security configuration by admin	human-deliberate	malicious insider(s)	(1) Strong network security	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Rubin, Avi (2002) "Security Considerations for Remote Electronic Voting over the Internet", Floram Park, NJ: AT&T Labs – Research, Retrieved from http://avirubin.com/e-voting.security.html
243	Ti34	Insert manipulated transaction	Attack on a network device allows attacker to insert a manipulated message into a voting session.	Network device: poor network security, poor security configuration by admin	human-deliberate	malicious insider(s)	(1) Strong network security (2) Auditing	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Jefferson, D., A. D. Rubin, B. Simons, and D. Wagner. (2004). Analyzing Internet voting security.Communications of the ACM, 47(10), 59-64.
244	Ti36	Malicious admin account	Attacker compromises voting server security by establishing an admin account.	Network server: admin susceptibility to bribery and coercion	human-deliberate	malicious insider(s)	(1) Strong network security (2) Strong legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Rubin, Avi (2002) "Security Considerations for Remote Electronic Voting over the Internet", Floram Park, NJ: AT&T Labs – Research, Retrieved from http://avirubin.com/e-voting.security.html
245	Ti38	Inject malware	Install malicious software on a device so that it can later execute on that device.	Network server: poor network security, poor security configuration by admin	human-deliberate	malicious insider(s)	(1) High Assurance software (2) Two person integrity (3) Strong network security (4) Strong legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Rubin, Avi (2002) "Security Considerations for Remote Electronic Voting over the Internet", Floram Park, NJ: AT&T Labs – Research, Retrieved from http://avirubin.com/e-voting.security.html
246	Ti39	Create the malware	Design, code, and test the software artifact that will be used to attack the voting system.	Not modeled: access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	human-deliberate	malicious insider(s)	None provided in reference.	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Rubin, Avi (2002) "Security Considerations for Remote Electronic Voting over the Internet", Floram Park, NJ: AT&T Labs – Research, Retrieved from http://avirubin.com/e-voting.security.html Jefferson, D., A. D. Rubin, B. Simons, and D. Wagner. (2004). Analyzing Internet voting security.Communications of the ACM, 47(10), 59-64.
247	Ti41	Flip votes	Create software that will record a vote that is different from the voter's selection.	Not modeled: access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	human-deliberate	malicious insider(s)	(1) High Assurance Software (2) Effective auditing (3) Auditing	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Rubin, Avi (2002) "Security Considerations for Remote Electronic Voting over the Internet", Floram Park, NJ: AT&T Labs – Research, Retrieved from http://avirubin.com/e-voting.security.html
248	Ti44	Delete races	Create software that deletes contests from the ballot that is presented to the voter.	Not modeled: access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption	human-deliberate	malicious insider(s)	(1) High Assurance Software (2) Effective auditing (3) Auditing	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007, Retrieved from http://election.dos.state.fl.us/voting-systems/pdf/SAITreport.pdf
249	Ti60	Discard the ballot	Malware terminates the session, convincing the voter that the ballot was cast, but without casting the ballot.	Remote voter: susceptibility to bribery, coercion, and deception	human-deliberate	malicious insider(s)	(1) High assurance software (2) Auditing	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Rubin, Avi (2002) "Security Considerations for Remote Electronic Voting over the Internet", Floram Park, NJ: AT&T Labs – Research, Retrieved from http://avirubin.com/e-voting.security.html
250	Ti69	Receive, mark, return their ballot		Remote voter: personnel training or integrity issues; faulty authentication	human-deliberate	malicious outsider(s)	None provided in reference.	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
251	Ti71	Vote attribution attack	Type of attack that is enabled by a voter being able to prove how they vote.	Remote voter: susceptibility to bribery and coercion	human-deliberate	malicious outsider(s)	(1) Receipt-free voting system	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
252	Ti73	Recruit brokers	Vote buyer recruits brokers to reach move voters and to protect himself from legal ramifications.	Remote voter: susceptibility to bribery and coercion	human-deliberate	malicious outsider(s)	(1) Strong legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
253	Ti74	Identify prospective vote sellers	Vote buyer engages voters that are willing to sell their votes.	Remote voter: susceptibility to bribery and coercion	human-deliberate	malicious outsider(s)	(1) Strong legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Estep, Bill, "Clay Co. vote-buying investigation keeps expanding" Lexington Herald-Leader, Monday, May. 18, 2009 http://www.kentucky.com/181/story/799167.html
254	Ti75	Send instructions	Vote buyer communicates the actions that the vote sellers take to accomplish the transaction.	Remote voter: susceptibility to bribery and coercion	human-deliberate	malicious outsider(s)	(1) Legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
255	Ti78	Voter coercion	Attacker influences voter via threat or intimidation.	Remote voter: susceptibility to bribery and coercion	human-deliberate	malicious outsider(s)	(1) Voter training (2) Receipt-free voting system (3) Strong legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Jefferson, D., A. D. Rubin, B. Simons, and D. Wagner. (2004). Analyzing Internet voting security.Communications of the ACM, 47(10), 59-64. Mote, C. D. Jr. (2002).Report of the national workshop on Internet voting: issues and research agenda. ACM International Conference Proceeding Series, 129, 1-59.
256	Ti79	Pay voter not to vote	Attacker pays a voter to not cast a ballot at all.	Remote voter: susceptibility to bribery and coercion	human-deliberate	malicious outsider(s)	(1) Strong legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Hasen, Richard L., "Vote Buying" California Law Review, Vol. 88, p. 1323, October 2000; Loyola-LA Legal Studies, Retrieved from http://ssrn.com/abstract=257564.

Index ID	Source ID	Threat Vector	Threat Event	Vulnerability	Threat Agent Category	Threat Agent(s)	Potential Mitigation	Source	Reference
257	Ti80	Compromise cryptography	Identify and exploit weaknesses in the system's cryptography implementation.	Network device, server, pc: attacker access to tools, techniques, and information	human-deliberate	malicious insider(s)	(1) High assurance software	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007, Retrieved from http://election.dos.state.fl.us/voting-systems/pdf/SAITreport.pdf
258	Ti81	Compromise key management	Identify and exploit weaknesses in the system's key management process.	Network device, server, pc: attacker access to tools, techniques, and information	human-deliberate	malicious insider(s)	(1) High assurance software	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007, Retrieved from http://election.dos.state.fl.us/voting-systems/pdf/SAITreport.pdf
259	Ti82	Compromise randomness	Identify and exploit weaknesses in the system's random number generation.	Network device, server, pc: attacker access to tools, techniques, and information	human-deliberate	malicious insider(s)	(1) High assurance software	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007, Retrieved from http://election.dos.state.fl.us/voting-systems/pdf/SAITreport.pdf
260	Ti83	Other protocol compromise	Identify and exploit weaknesses in other security protocols.	Network device, server, pc: attacker access to tools, techniques, and information	human-deliberate	malicious insider(s)	(1) High assurance software	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007, Retrieved from http://election.dos.state.fl.us/voting-systems/pdf/SAITreport.pdf
261	Ti85	Register as a fictitious person	Use a fake id to register as a fictitious voter	Authenticate voter: soft verification process	human-deliberate	malicious outsider(s)	Verification process should be improved; make use of machine that can differentiate between fake and original Id's	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
262	Ti107	Manipulate ballot definition	Attacker alters the ballot definition to manipulate voter selections.	Votable ballot: faulty validation process; personnel training or integrity issues	human-deliberate	malicious insider(s)	(1) High assurance software (2) Legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	NIST Andrew Regenscheid and Nelson Hastings, A Threat Analysis on UOCAVA Voting Systems. NISTIR 7551, December 2008, Retrieved from http://vote.nist.gov/uocava-threatanalysis-final.pdf
263	Ti109	Manipulate voted ballots	Changing selections on voted ballots.	Marked ballot: faulty validation process; personnel training or integrity issues	human-deliberate	malicious insider(s)	(1) High assurance software (2) Legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Yasinsac, Alec, Breno de Medeiros, David Gainey, John Kerski, Zachary Hartley, Ryan Walega, and Michael Gerke, " Software and Security Review for Elections Systems and Software iVotronic Firmware Versions 9.1.8.0 and 9.2.0.0", Supplemental Report, For the Florida Department of State, August 14, 2007. Yasinsac, Alec, D. Wagner, M. Bishop, T. Baker, B. de Medeiros, G. Tyson, M. Shamos, and M. Burmester, "Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware, Final Report", Security and Assurance in Information Technology (SAIT) Laboratory, Florida State University, February 23, 2007. Yasinsac, Alec, John Kerski, David Gainey, Michael Gerke, Kristine Amari, and Donald Newell, "Software Review and Security Analysis of the Diebold Voting Machine Software", TSX Supplement, For the Florida Department of State, September 28, 2007.
264	Ti114	Human error mis-mark	Voter marks the wrong selection indicator, i.e. does not properly match the selection indicator to their preferred choice.	Eligible voter: voting machine interface	human-unintentional	voter	(1) Voter training	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Yasinsac, A. and Bishop. M. (2008). The Dynamics of Counting and Recounting Votes.IEEE S&P Magazine, 6(3), 22-29. Yasinsac, A. and Bishop, M. (2008). Of Paper Trails and Voter Receipts.Proceedings of the 41st Hawaii International Conference on System Sciences.
265	Ti115	Ballot design flaw	The ballot structure or presentation causes voters to make selection errors.	Votable ballot: faulty testing process; personnel training or integrity issues	human-unintentional	local election official	(1) Rigorous ballot design testing	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007, Retrieved from http://election.dos.state.fl.us/voting-systems/pdf/SAITreport.pdf
266	Th119	Unlikely voters	Make lists of voters very unlikely to vote this election	Voter lists: access to voter lists and ability to determine voters not likely to vote	human-deliberate	malicious outsider(s)	chain of custody controls on voter registration lists, if not public information	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
267	Th120	Assign impersonator to voter	Supply attackers with information about unlikely voter (e.g., name and gender)	Poll workers, authenticate voter: poll workers fooled by unknown attacker with valid voter information	human-deliberate	malicious outsider(s)	physical and environmental protection, audit and accountability, identification and authentication	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
268	Th124	Register as an housemate	Recruit registers impersonators as housemates / roommates	People being recruited: corruptibility or vulnerability of recruits	human-deliberate	malicious outsider(s)	strengthen the controls in the ElectionSystem	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
269	Th126	Recruit cell captains	Recruit cell captains	People being recruited: corruptibility or vulnerability of political loyalists of political leader	human-deliberate	malicious insider(s)	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
270	Th127	Motivate cell captains	Educate and motivate cell captains in deniable ways	People being recruited: insulation of lead attacker from discovery	human-deliberate	malicious insider(s)	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
271	Th128	Recruit attackers	Cell captains recruit more attackers	Voters: corruptibility of potential impersonators; resources of attackers	human-deliberate	malicious insider(s)	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
272	Th130	Supply rewards	Cell captain provides all required rewards out of own pocket	Voters: susceptibility of insiders to bribery and corruption	human-deliberate	malicious insider(s)	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and poll workers, physical and environmental protection, limiting access to polling place and providing polling place patrols	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
273	Th133	Force least-objectionable choice	Force least-objectionable candidate voting	Votable ballot: lack of acceptable candidates running for office	human-unintentional	local election official	system and information integrity-9, allow for "none-of-the above" choices in contests	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	VNOTA (2006) Vote for None of the Above, Retrieved from http://nota.org

Index ID	Source ID	Threat Vector	Threat Event	Vulnerability	Threat Agent Category	Threat Agent(s)	Potential Mitigation	Source	Reference
274	Th135	Tamper with poll book	Tamper with poll book to add no-show voters	Poll book: unsecured poll book; lack of supervision	human-deliberate	malicious insider(s)	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
275	Th137	Falsely reject voter registration	Falsely reject voter claiming they are not registered	Checking, check poll book, authenticate voter: unwillingness or inability of voters to appeal poll workers' decisions	human-deliberate	malicious insider(s)	provide appeal process for oversight of poll worker	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
276	Th139	Use poor audit process	Use poor auditing processes and procedures	Election audit, validate precinct results: poor auditing practices or procedures	human-deliberate; human-unintentional	malicious insider(s); local election official	revise auditing practices or procedures to audit manipulation	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
277	Th148	Discard / destroy markedballots	Use private access to discard or destroy a box of markedballots (fail to replace)	Precinct close out, deliver to jurisdiction, etc. any activity where one person or a group of collaborating people, can gain private access to a physical ballot box.: for any system based on physical ballots, each ballot is a constrained data item (cdi). it is a well known security principle that the	human-deliberate	malicious insider(s)	Ballot accounting, chain of custody, personnel screening	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
278	Th153	Vote using more than one method	Vote early and regular, or absentee and provisional as a form of ballot box stuffing	Authenticate voter remote, voter list, voter information, authenticate voter, authentication rules, jurisdiction: inability to or failure to cross-check poll books for different voting methods within a single place (jurisdiction)	human-deliberate	malicious outsider(s)	system and information integrity-improve integrity of voter lists, identification and authentication-authenticate voters	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
279	Th154	Vote in more than one place	Vote in two neighboring states or multiple precincts with registrations in more than one place	Voter list, voter information, authenticate voter, authentication rules, jurisdiction: inability to or failure to cross-check voter lists across multiple jurisdictions	human-deliberate; human-unintentional	malicious outsider(s); voter	system and information integrity-improve integrity of voter lists, identification and authentication-authenticate voters	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
280	Th157	By undoing voter marks	Erase or otherwise undo voter's mark on ballot	Marked ballots, especially prior to counting: insider access to ballots; lack of oversight / chain of custody of ballots	human-deliberate	malicious outsider(s)	ballot chain of custody procedures; post-election review of ballots	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
281	Th165	Insert unauthorized physical ballots into the ballot box	Insert unauthorized physical ballots into the ballot box	Commit ballot: cannot bind a paper ballot to a voter. for a physical ballot box with a slot, a voter may stack several ballots and insert them at the same time.	human-deliberate	malicious insider(s)	Ballot box attendant, probably not particular effective	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
282	Th168	By marking ballot	Alter markedballots by marking selections that either exploit undervotes or cause overvotes	Precinct close out, deliver to jurisdiction, etc. any activity where one person or a group of collaborating people, can gain private access to physical ballots.: paper ballots have no "final form" status. that is, they can be marked after the voter has cast the ballot. for any system based on physica	human-deliberate	malicious outsider(s)	establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
283	Th169	Selectively recount	Selectively recount by county or precinct	Validate total, recount: election law	human-deliberate	malicious insider(s)	election law, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
284	Th170	With physical damage	Tamper with ballots by doing physical damage	One voter: unobserved physical access to paper	human-deliberate	malicious insider(s)	physical access controls	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
285	Th174	Mislead about committing ballot	Mislead voters about correct commitment of ballot	One voter: poll workers have discretion to instruct voters and voters do not tend to read informative signs	human-deliberate	malicious outsider(s)	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
286	Th251	With invalidating marks	Alter physical ballots by making illegal marks that will invalidate ballots during hand count or hand recount.	Precinct close out, deliver to jurisdiction, etc. any activity where one person or a group of collaborating people, can gain private access to physical ballots.: paper ballots have no "final form" status. that is, they can be marked after the voter has cast the ballot. for any system based on physica	human-deliberate	malicious insider(s)	establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
287	Th252	Stuff during canvass or recount	Inject ballot box (of physical ballots) during canvass or recount	Validate total, process remote ballots: after the election, during the validate process, ballot boxes may be placed where they will be found in storage rooms, elections officials' cars, etc.	human-deliberate	malicious insider(s)	Ballot watermarking, ballot accounting, registration reconciliation	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Chan, Sharon P. (2008), "Tuesday election a huge test for King County after 2004 mistakes," Seattle Times, October 31, 2008, Retrieved from http://seattletimes.nwsource.com/html/governo rsrace/2008333581_kingelexoffice31m.html on March 8, 2009.
288	Th253	Disallow legitimate ballots	Challenge the authenticity of legitimate ballots, including erroneous authenticity challenges, disqualifying marks, etc.	Validate total, recount: cannot bind a ballot to a voter	human-deliberate	malicious insider(s)	planning: establish clear and effective rules for ballot adjudication; personnel security: implement personnel sanctions; awareness and training	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
289	Th254	Manipulate duplicate ballots	Alter the ballot to be counted, or mishandle to allow both the original and duplicate to be counted	Ballot box accounting, recount, validate jurisdiction results, ballot delivery: marked ballots cannot be bound to the voter, so detecting multiple votes by / for the same voter is difficult to detect and / or prevent.	human-deliberate	malicious insider(s)	personnel management, chain of custody rules	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
290	Th405	Confuse voters with poor ballot design	Poor ballot design that confuses or misleads voters during voting process, or fails to prevent voter errors in marking ballot	Validate ballot style, checked in voter: weak reviewing process of a ballot design	human-deliberate	malicious insider(s)	use ballot design checklist, implement usability testing, review and amend election laws	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Norden, Lawrence, Kimball, David, Quesenbery, Whitney, and Chen, Margaret (2008) "Better Ballots." July 20 2008, Retrieved from Brennan Center for Justice, http://www.brennancenter.org/content/resourc e/better_ballots
291	Th503	Selectively challenge voters	Selectively challenge voters, such as "undesirable" voters in polling place	Voter check in: ability of poll workers or collusions of poll workers to control voter checking; lack of oversight	human-deliberate	malicious insider(s)	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
292	Th505	With phony voter assistant	Assist voter at precinct to verify bought vote; voter requests assistance in order to earn reward from assistant	Sign poll book, validate precinct results: failure to authenticate voter's assistant; failure to detect unusual patterns of assistance (same assistant, higher than normal assistance)	human-deliberate	malicious insider(s)	audit and accountability audit precinct results and investigate any unusual voting patterns, such as a high percentage of voter assistance or repeated assistance by the same assistant; prevent by asking voter for reason assistance needed	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
293	Th506	By splitting contests up	Split candidates for the same office onto different pages or columns	Validate ballot style: weak reviewing process of a ballot design	human-deliberate	malicious insider(s)	* use ballot design checklist, implement usability testing, review and amend election laws (* note the above also applies to thread id # 557 - 568), list all candidates for the same race on the same page in the same column	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Norden, Lawrence, Kimball, David, Quesenbery, Whitney, and Chen, Margaret (2008) "Better Ballots." July 20 2008, Retrieved from Brennan Center for Justice, http://www.brennancenter.org/content/resourc e/better_ballots
294	Th507	Falsely announce results	Falsely announce tabulation results; announcement of tabulation result ignoring actual ballots	Unofficial results, report results: dependence on key election official(s) with centralized power to announce / certify result	human-deliberate	malicious insider(s)	security-related activity planning, chain of custody of results of the tabulation process, including access control policies and procedures, separation of duties, physical access controls, auditing and accountability, such as verifying results against tabulated; incident monitoring and reporting; making whole process more transparent to media and public	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.

Index ID	Source ID	Threat Vector	Threat Event	Vulnerability	Threat Agent Category	Threat Agent(s)	Potential Mitigation	Source	Reference
295	Th508	By spreading response options	Place response options on both sides of candidate names	Validate ballot style: weak reviewing process of a ballot design	human-deliberate	malicious insider(s)	place response options (such as fill-in-the-ovals) in a consistent place on the ballot, such as one side of candidate names or ballot or ballot question choices	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Norden, Lawrence, Kimball, David, Quesenbery, Whitney, and Chen, Margaret (2008) "Better Ballots." July 20 2008, Retrieved from Brennan Center for Justice, http://www.brennancenter.org/content/resource/better_ballots
296	Th516	With complex instructions	Fail to write short, simple instructions	Validate ballot style: weak reviewing process of a ballot design	human-deliberate	malicious insider(s)	write short instructions with simple words	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Norden, Lawrence, Kimball, David, Quesenbery, Whitney, and Chen, Margaret (2008) "Better Ballots." July 20 2008, Retrieved from Brennan Center for Justice, http://www.brennancenter.org/content/resource/better_ballots
297	Th521	By keeping disqualified candidates	Leave columns or rows for disqualified candidates	Validate ballot style: failure to remove disqualified candidates from ballot; failure to inform voters of disqualified candidates	human-deliberate	malicious insider(s)	remove the entire column or row for any candidate or party that has been withdrawn or disqualified (not just the candidate or party name)	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Norden, Lawrence, Kimball, David, Quesenbery, Whitney, and Chen, Margaret (2008) "Better Ballots." July 20 2008, Retrieved from Brennan Center for Justice, http://www.brennancenter.org/content/resource/better_ballots
298	Th522	With inconsistent formats	Inconsistently design ballots in formatting and style	Validate ballot style: weak reviewing process of a ballot design	human-deliberate	malicious insider(s)	use consistent format and style for every contest and voting action	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Norden, Lawrence, Kimball, David, Quesenbery, Whitney, and Chen, Margaret (2008) "Better Ballots." July 20 2008, Retrieved from Brennan Center for Justice, http://www.brennancenter.org/content/resource/better_ballots Frisina, Laurin, Herron, Michael C., Honaker, James, Lewis, Jeffrey B. (2008) "Ballots Formats, Touchscreens, and Undervotes: A Study of the 2006 Midterm Elections in Florida", Election Law Journal: Rules, Politics, and Policy. March 2008, 7(1): 25-47. DOI: 10.1089/elj.2008.7103
299	Th523	Switch box during transport	Substitute ballot box (add, discard, change ballots) during transport to central location	One voter, ballot delivery: failure to take the details of the person transferring the votes to the central location	human-deliberate	malicious insider(s)	physical and environmental protection-Delivery and Removal, , personnel security-Third Party personnel security	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
300	Th524	By omitting useful shading	Omit shading to help voters differentiate between voting tasks	Validate ballot style: weak reviewing process of a ballot design	human-deliberate	malicious insider(s)	shade certain text, such as office name to help voters to differentiate between voting tasks	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Norden, Lawrence, Kimball, David, Quesenbery, Whitney, and Chen, Margaret (2008) "Better Ballots." July 20 2008, Retrieved from Brennan Center for Justice, http://www.brennancenter.org/content/resource/better_ballots
301	Th528	By subverting ballot rotation	Tamper with ballot design so that ballot rotation is subverted	Votable ballots: failure of tests to detect all anomalies	human-deliberate	malicious insider(s)	establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
302	Th530	By expected voting pattern	Select a precinct that follows a particular voting pattern making it easier to carry out the attack	Polling place: increasing availability (i.e. web-based) of election results reported by precinct, for which attacker can select a precinct based on the voting pattern the precinct follows	human-deliberate	malicious insider(s)	personnel security, including Position Categorization and Personnel Sanctions	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
303	Th531	Alter results transmission	Results will be transmitted to county elections department on the election night. there are chances that the precinct results might be altered before transmitting them to the elections department.	Precinct result: attacker can alter the transmission of precinct results by adding a counterfeit ballot box, ignoring the provisional votes etc.,	human-deliberate	malicious insider(s)	security-related activity planning, chain of custody of results of the tabulation process, including access control policies and procedures, physical access controls, auditing and accountability; incident monitoring and reporting; making whole process more transparent to media and public	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
304	Th532	Subvert reported results	Impersonate poll worker reporting preliminary precinct results; malicious outsider threatens the poll worker to disclose false results to the jurisdiction so as to change the election outcome.	Get precinct results flow chart: poll worker impersonation to alter the precinct result	human-deliberate	malicious insider(s)	security-related activity planning, chain of custody of results of the tabulation process, including access control policies and procedures, physical access controls, auditing and accountability; incident monitoring and reporting; making whole process more transparent to media and public	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
305	Th549	Mislead w/phony ballot change	Mislead voters by announcing phony last-minute ballot change	Eligible voter, signed in voter: susceptibility of voters to believe what was being informed by the poll worker	human-deliberate	malicious insider(s)	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
306	Th550	Mislead w/one party only ruse	Mislead voters by announcing that only one party is allowed to vote	Eligible voter, signed in voter: susceptibility of voters to believe what was being informed by the poll worker	human-deliberate	malicious insider(s)	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
307	Th552	Modify electionartifacts	Modify poll books for audit; modify logbooks and log data used in audit	Check poll book for authenticate voter, poll worker logs for precinct closeout: lack of management oversight over poll worker, election-official, auditor	human-deliberate	malicious insider(s)	audit monitoring, analysis, and reporting	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
308	Th554	Subvert audit data	Poll worker changes audit data	Precinct audit data: lack of management oversight over poll worker, election-official, auditor	human-deliberate	malicious insider(s)	audit monitoring, analysis, and reporting	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
309	Th555	Mishandle audit batch	Swap, replace, hide, mislay, or mislabel batch of audit data; e.g. poll worker or election-official incorrectly labels batch of audit data	Precinct audit data: unintentional -vulnerability to human error due to carelessness; intentional - mislabel batch to cover fraud from being detected	human-deliberate; human-unintentional	malicious insider(s); malicious outsider(s); voter; local election official; mail employee; ISP technician	audit monitoring, analysis, and reporting	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
310	Th566	Delay voters with poor assistance	Delay voters by failing to properly assist	Voter: poor poll worker performance; lack of oversight	human-deliberate; human-unintentional	malicious insider(s); local election official	planning, including rules of behavior; poll worker awareness and training; and personnel policies, including sanctions for poor performance	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
311	Th603	Add fraudulent result data	Inject fake votes to a back-end tabulating authority by impersonating a legitimate precinct	Marked ballots, especially prior to counting: poor physical security ballot boxes	human-deliberate	malicious insider(s)	increase physical security;	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Kohno, Tadayoshi, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach. "Analysis of an Electronic Voting System," February 24, 2004, Retrieved from http://avirubin.com/vote.pdf
312	Th604	Destroy registered cards	A third party working on behalf of voter registration encourages people to register and after the registration process destroy or discard their cards	Registered cards: lack of management oversight over third party	human-deliberate	malicious insider(s)	Get the details from third party and mail the voter Id's to the votes instead asking third party to handover the id's.	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Ballotpedia (2008) Illegal third-party registration conduct, October 22, 2008, Retrieved from http://ballotpedia.org/wiki/index.php/Illegal_third-party_registration_conduct.
313	Th605	Falsely challenge voters on target list	Creating a target list of voters to challenge and falsely question voters' right to vote	Eligible voters; (no suggestions): disclosing information of voters	human-deliberate	malicious insider(s)	chain of custody for voter lists, including access control policies	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Levitt, Justin and Allison, Andrew (2007) A Guide to Voter Caging, Brennan Center For Justice, Jun 29, 2007, Retrieved from http://www.brennancenter.org/content/resource/a_guide_to_voter_caging/
314	Th608	Persuade voter selections	Persuade the voter to vote a certain way	Voting activity: lack of decisiveness in the voter, lack of management oversight over poll workers	human-deliberate	malicious outsider(s)	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.

Federal Voting Assistance Program
Comparative Risk Analysis of the Current UOCAVA Voting System and an Electronic Alternative Report
Vulnerability-Threat Database (VTDb)

Index ID	Source ID	Threat Vector	Threat Event	Vulnerability	Threat Agent Category	Threat Agent(s)	Potential Mitigation	Source	Reference
315	Th619	Make a non-cash payment	Use drugs or alcohol as payment for votes; attacker promises and exchanges drugs or alcohol in exchange for voting for attacker's candidates	Eligible voter, signed in voter: susceptibility of voters with substance abuse to bribery	human-deliberate	malicious outsider(s)	maintain ballot secrecy	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Campbell, Tracy (2006) Deliver the Vote: A History of Election Fraud, An American Political Tradition-1742-2004. New York: Perseus Books Group: Palgrave Macmillan. pp. 144, 282. Estep, Bill (2009) "Former Clay official to change plea in vote-buying case," Lexington Herald-Leader, May 29, 2009, Retrieved from http://www.kentucky.com/2009/05/29/811016/former-clay-official-to-change.html
316	Th620	Pay voters cash	Pay the "market" rate for a vote in direct cash payment	Eligible voter, signed in voter: susceptibility of voters to bribery	human-deliberate	malicious outsider(s)	prosecute voters who sell their vote; throw out illegal votes; maintain ballot secrecy	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Campbell, Tracy (2006) Deliver the Vote: A History of Election Fraud, An American Political Tradition-1742-2004. New York: Perseus Books Group: Palgrave Macmillan. pp. 278, 283
317	Th622	That exploit electoral college rules	Use winner-take-all electoral college design to tempt a selective attack in a tight presidential race	Voting system, election system: availability of polling data enables careful calculation of the number of votes needed to win, which can be leveraged by the winner-take-all electoral design	human-deliberate	malicious insider(s)	recommend that states award electoral votes in proportion to popular vote	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Campbell, Tracy (2006) Deliver the Vote: A History of Election Fraud, An American Political Tradition-1742-2004. New York: Perseus Books Group: Palgrave Macmillan. p. 337
318	Th628	Promise to pay	Promise payment later or promise payment based on subsequent verifiability of voter's carry out attacker's voting demands	Voters: susceptibility of voters to bribery	human-deliberate	malicious outsider(s)	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and poll workers	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
319	Th632	Alter voter's vote	Alter voter's vote in polling place	Voter, one voter: poll worker discretion to instruct voter; voter's lack of understanding	human-deliberate	malicious insider(s)	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	LTM-USA Delivery-01 (2009) LTM Election Threat Models, Lazarus Technology Mentoring, Inc.
320	Th633	Threaten other than polls	Perform insider threat at other than polling place	Contest artifacts: insider access to contest artifacts	human-deliberate	malicious outsider(s)	election law, ballot chain of custody controls, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
321	Th634	Access ballots to alter votes	Access ballots, either marked, provisional, or assisted, to alter votes	One voter: poll worker discretion to instruct voter; voter's lack of understanding	human-deliberate	malicious insider(s)	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
322	Th636	Collect ballots from voters	Collect ballots from legitimate voters	One voter: poll workers have discretion to instruct voters and voters do not tend to read informative signs	human-deliberate	malicious outsider(s)	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
323	Th637	Tamper with ballots	Tamper with ballots before they are collected	Votable or marked ballot: lack of oversight	human-deliberate	malicious insider(s)	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
324	Th638	Obtain ballot of assisted voter	Subvert votes of voters needing assistance	Votable or marked ballot: vulnerability of voter in need of assistance to the abuses of malicious poll worker	human-deliberate	malicious insider(s)	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
325	Th639	Form inside attack team	Form attack team of one or more attackers with insider privileges	Voting system: insider access, availability and willingness of insiders, difficulty in detection	human-deliberate	malicious insider(s)	personnel security, awareness and training, incident response, physical and environmental protection	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
326	Th640	Obtain markedballot	Create plausible reason to obtain markedballot	One voter: poll worker discretion to instruct voter; voter's lack of understanding	human-deliberate	malicious insider(s)	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
327	Th644	Execute insider threat	Execute insider threat	Voting system, election artifacts: insider access, availability and willingness of insiders, difficulty in detection	human-deliberate	malicious insider(s)	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
328	Th646	Subvert rules for determining voter intent	Subvert rules for determining voter intent	Contest results, candidate, political parties: lack of transparency, poor verification process	human-deliberate	malicious insider(s)	election law, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
329	Th647	Stuff ballots after closing	Stuff ballot box after the polls close	Ballots, ballot box: access to ballots, ballot box; lack of management oversight	human-deliberate	malicious insider(s)	election law, ballot chain of custody controls, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
330	Th648	Threaten ballots	Perform threats on votableballots or markedballots	Votable ballots: access to ballots, difficulty of detection	human-deliberate	malicious insider(s)	establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
331	Th649	Subvert tabulated results	Threaten results of tabulation process	Election artifacts: dependence on key election official(s) with centralized power to announce / certify result	human-deliberate	malicious insider(s)	security-related activity planning, chain of custody of results of the tabulation process, including access control policies and procedures, physical access controls, auditing and accountability; incident monitoring and reporting; making whole process more transparent to media and public	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
332	Th651	Publish invalid sample ballots	Publish sample ballots different from actual ballots	Validate ballot style: weak reviewing process of a ballot design	human-deliberate; human-unintentional	malicious insider(s); local election official	None provided in reference.	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
333	Th1003	Lose ballots by accident	Unintentionally lose or misplace ballots, including close-polls filing errors	Ballots: poor poll worker performance; lack of oversight	human-unintentional	local election official	awareness and training awareness and training,; personnel security personnel policies; audit and accountability audit and accountability; information integrity accuracy tests; planning	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
334	Th1004	Stuff, swap, or lose the ballot box	Count ballots/batches of ballots more than once, by accident	Poll workers, voters: poor planning	human-deliberate	malicious insider(s)	awareness and training awareness and training,; personnel security personnel policies,; audit and accountability audit and accountability; information integrity accuracy tests; planning	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
335	Th1010	Cast multiple votes	A legalvoter votes more than once; ballot box stuffing by the voter	Voting: inability of voting system to capture duplicate votes by a voter	human-deliberate	malicious outsider(s)	system and information integrity, identification and authentication	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.

Index ID	Source ID	Threat Vector	Threat Event	Vulnerability	Threat Agent Category	Threat Agent(s)	Potential Mitigation	Source	Reference
336	Th1011	Pay	Motivate voter with pay	Voter: human susceptibility to being bribed	human-deliberate	malicious outsider(s)	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and poll workers	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
337	Th1012	Verify bought vote	Assess voter compliance with direction	Voter: inability to prevent voter attribution	human-deliberate	malicious outsider(s)	prevent voter attribution with ballot secrecy, preventing stray marks, and making sure that voter assistance is legitimately needed	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
338	Th1013	With encoded stray marks	Make stray ballot mark for voter attribution	Votable ballot: ability of voter to mark ballot freely	human-deliberate	malicious outsider(s)	use ballot marking that prevents stray marks; clear plastic ballot sleeve; investigate unusual patterns of write-ins	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
339	Th1083	Disrupt operations	Disrupt operations	Polling place, voting: exposure to natural or environmental events, fragility of ballots, susceptibility of voters to threats and intimidation	accidental	natural; environmental; human-created collateral	disaster planning, contingency planning, physical and environmental protection, incident response, and personnel security	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
340	Th1084	Disruption from natural events	Voting system failures attributable to natural events	Polling place, voting: exposure to natural events	accidental	natural	disaster recovery planning; physical and environmental protection policies, incident response with coordination among government entities	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Rackleff, Robert (2007) "Voters of Hurricane Katrina," Carnegie Reporter, Vol. 4 No. 2, Spring 2007, Carnegie Corporation of New York.
341	Th1085	Natural disaster	Polling place hit by tornado, hurricane, tsunami, flood, earthquake, landslide, wildfire, lightening, strike, etc	Polling places, displaced voters: exposure to natural or accidental events	accidental	natural	disaster recovery planning; hurricane and flood protection; contingency planning; incident response with coordination among government entities	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Rackleff, Robert (2007) "Voters of Hurricane Katrina," Carnegie Reporter, Vol. 4 No. 2, Spring 2007, Carnegie Corporation of New York.
342	Th1087	Disruption from environmental events	Disruption from environment al events	Polling place: exposure to environment events	accidental	environmental	disaster recovery planning; physical and environmental protection policies, coordination with other government entities	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
343	Th1088	Environmental failures	Polling place facilities failures including power failure, electrical fire, burst water pipes	Polling place: exposure to environment events	accidental	natural; environmental; human-created collateral	disaster recovery planning; physical and environmental protection policies, coordination with other government entities	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
344	Th1089	Hazardous accidents	Polling place access impaired by nearby hazards including chemical spill, power wire fall, gas main explosion	Polling place, poll workers, voters: exposure to environment events; exposure to danger	accidental	environmental	disaster recovery planning; physical and environmental protection policies, coordination with other government entities	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
345	Th1090	Disruption from human-created events	Disruption from human-created events	Polling place: fragility of ballots, mishandling	accidental	human-created collateral	planning; physical and environmental protection, access control	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
346	Th1094	Discourage voter participation	Discourage voter participation	Voter: susceptibility of voters to violence, intimidation, fear	human-deliberate	malicious outsider(s)	awareness and training, planning, contingency planning, incident response, physical and environmental protection	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
347	Th1096	Threaten personal violence	Threaten personal violence, such as in blackmailing a voter to be a no-show or to vote for attacker's candidate; attacker focuses on a particular voter threatens him to vote against his will	Eligible voter: susceptibility of voters to intimidation; lack of voter privacy	human-deliberate	malicious outsider(s)	planning, strengthen laws against such crimes; physical and environmental security; voter privacy	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Van Acker, Bernard (2004), Remote e-Voting and Coercion: a Risk-Assessment Model and Solutions, 2004, Retrieved from http://subs.emis.de/LNI/Proceedings/Proceedings47/Proceeding.GI.47-6.pdf
348	Th1097	Threaten mass violence	Violence to prevent voting, (i.e., bomb scare, mail contamination scare (do not open mail), perhaps even targeting areas (by zip code)	Voters: voters' fear for their safety	human-deliberate	malicious outsider(s)	contingency planning contingency planning, incident response incident response, physical and environmental protection physical and environmental protection	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Foxnews.com (2005), "Riot, bomb scare at Australian polls," Associated Press, Fox News Network LLC, January 29, 2005, Retrieved from http://www.foxnews.com/story/0,2933,145763,00.html
349	Th1098	Commit an act of terror	Commit an act of terror	Voters, election officials, voting equipment: exposure to terrorist acts of violence	human-deliberate	malicious outsider(s)	physical and environmental protection: arms and ammunitions should not be allowed in the polling area. Unclaimed items should be continuously checked. Regular police patrolling required.	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
350	Th1110	Commit hand tabulation errors	Experience un-detected tabulation errors	Accumulation, retabulation, reconcile voter feedback: fatigue, unclear counting rules, misinterpret counting rules	human-unintentional	local election official	start counting well before polls close; use dedicated counting team; have new hires work under trainers; take breaks after each hour of counting; use techniques not prone to error; checking	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
351	Th1112	In straight-party vote tabulation	Due to use of incorrect rules for straight-party vote interpretation	Accumulation, retabulation, reconcile voter feedback: unclear counting rules, misinterpret counting rules	human-deliberate	malicious insider(s)	logic and accuracy tests that include straight-party voting tests that test actual vs. expected counts	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Independent Political Report (2008), "Update from Black Box Voting: Trouble with straight party voting and how you can help on Election Day," October 10, 2008, Retrieved from http://www.independentpoliticalreport.com/2008/10/update-from-black-box-voting-trouble-with-straight-party-voting-and-how-you-can-help-on-election-day/#more-3301. Jones, Doug W. (2005a) University of Iowa, Threats to Voting Systems, NIST workshop on Threats to Voting Systems, 7 October 2005, Gaithersburg, MD, Retrieved from http://vote.nist.gov/threats/papers/threats_to_voting_systems.pdf
352	Th1113	Due to improper tabulation technique	Due to use of incorrect selection of tabulation algorithm (e.g., irv variants)	Accumulation, retabulation, reconcile voter feedback: improper tabulation technique	human-unintentional	local election official	expert review of algorithm selection decision	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
353	Th1117	By omitting tallies from totals	Due to human error in omitting some tallies from vote total	Accumulation, retabulation, reconcile voter feedback: fatigue, unclear counting rules, misinterpret counting rules	human-unintentional	local election official	multi-person controls to verify correctness of human decisions	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
354	Th1118	By adding tallies multiple times	Due to human error in including some tallies from vote total multiple times	Accumulation, retabulation, reconcile voter feedback: fatigue, unclear counting rules, misinterpret counting rules	human-unintentional	local election official	multi-person controls to verify correctness of human decisions	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
355	Th1130	Misinform about overvoting / undervoting	Provide incorrect information about overvotes and undervotes	Voter: poor poll worker performance; lack of oversight	human-deliberate; human-unintentional	malicious insider(s); local election official	planning, including rules of behavior; poll worker awareness and training; and personnel policies, including sanctions for poor performance	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.

Index ID	Source ID	Threat Vector	Threat Event	Vulnerability	Threat Agent Category	Threat Agent(s)	Potential Mitigation	Source	Reference
356	Th1131	Allow undervotes without help	Allow undervotes without help	Voter: failure to assist voter in detecting undervotes	human-unintentional	local election official	voter education and training; clear ballot instructions that warn users about undervoting	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
357	Th1132	Allow overvotes without help	Allow overvotes without help	Voter: failure to assist voter in detecting overvotes	human-unintentional	local election official	voter education and training; clear ballot instructions that warn users about overvoting	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
358	Th1133	Encourage voter override	Encourage voter override of over/under-votes	Voter: poor poll worker performance; lack of oversight	human-deliberate; human-unintentional	malicious insider(s); local election official	planning, including rules of behavior; poll worker awareness and training; and personnel policies, including sanctions for poor performance	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
359	Th1135	Abuse ballots by accident	Unintentionally tamper with, mark, abuse ballots, including during close-polls operations	Voting: poor planning	human-unintentional	local election official	physical and environmental protection, media protection policy and procedures, personnel security, awareness and training	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
360	Th1136	Improperly select audit samples	Use improper methods of selecting the scope of audit	Election audit: difficulty in discovery	human-deliberate	malicious insider(s)	implement a more transparent and publicly observable random selection process, with clear written procedures or guidelines	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
361	Th1137	Select non-randomly	Use non-random selection methods	Audit data: poor auditing practices or procedures; failure to follow procedures; lack of management oversight over auditing practices	human-deliberate	malicious insider(s)	implement a more transparent and publicly observable random selection process, with clear written procedures or guidelines	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
362	Th1138	Use subverted selection method	Use selection methods subject to outside influence	Election artifacts: difficulty in detecting malware during computer use	human-deliberate	malicious insider(s)	access control, audit and accountability, identification and authentication, system and communications protection	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
363	Th1139	Ignore proper selections	Ignore randomly sampled audit units and audit something else	Validate precinct results: susceptibility of audit process to discretion of election officials	human-deliberate	malicious insider(s)	personnel security, audit and accountability	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
364	Th1140	Threaten election evidence	Election evidence includes electionartifacts, such as ballots, ballotpreparation data and artifacts, relevant pollbooks, physicalvoterecords, pollworker logs, voter feedback, etc.	Election artifacts: access to uncontrolled, accessible election artifacts	human-deliberate	malicious insider(s)	establish a chain of custody for all ElectionArtifacts used in audits; include separation of duties, access policies, audit logs, personnel policies, and media protections	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
365	Th1141	Commit auditing error	Human errors in following correct audit procedures, or overlooking errors	Ballot box accounting: election official has limited knowledge on discrepancies issues	human-unintentional	local election official	personnel security, including personnel sanctions; awareness and training: auditor training	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
366	Th1142	Compromise auditors	Suborn (bribe, threaten) auditors to intentionally misreport or suppress discrepancies between election results and audit results	Auditors: willingness of auditors to be bribed or coerced	human-deliberate	malicious insider(s)	personnel security, including sanctions against violators	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
367	Th1143	Subvert audit results	Attack audit-related process and data representing audit results	Election audit: lack of control over audit results	human-deliberate	malicious insider(s)	physical and environmental protection, media protection policy and procedures	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
368	Th1144	Modify deliberately	Deliberately modify audit data	Election artifacts: lack of management oversight over poll worker, election-official, auditor	human-deliberate	malicious insider(s)	establish a chain of custody on all ElectionArtifacts, including personnel security, physical and environmental protection, data protection policy and procedures	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
369	Th1145	Modify unintentionally	Modify audit data via poll worker error	Election artifacts: lack of management oversight over poll worker, election-official, auditor	human-unintentional	local election official	establish a chain of custody on all ElectionArtifacts, including personnel security, physical and environmental protection, data protection policy and procedures	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
370	Th1152	Mishandle electionartifacts	Swap, replace, hide, mislay, or mislabel electionartifacts containing election evidence	Election artifacts: access to election artifacts	human-deliberate	malicious insider(s)	implementation chain of custody on ElectionArtifacts including data protection policies	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
371	Th1153	Subvert tabulation	Intentionally commit errors in tabulation (i.e., counting)	Contest results: poor counting and verification processes, lack of transparency	human-deliberate	malicious insider(s)	election law, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
372	Th1155	Make mistakes in ballot adjudication	Make mistakes in ballot adjudication	Accumulation, retabulation, reconcile voter feedback: fallibility of human judgment; misinterpretation of rules; lack of oversight; human error; lack of voter being informed; inability of voter to protest	human-unintentional	local election official	planning: establish clear and effective rules for ballot adjudication; personnel security: implement personnel sanctions; awareness and training	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
373	Th1159	Commit vote fraud	Commit vote fraud attack	Voting, voters, ballots, poll workers, polling places: susceptibility of voters to being bribed or intimidated; lack of polling place security, availability of information to aid attack strategy	human-deliberate	malicious insider(s)	chain of custody controls on ballots, polling place security, multi-party observers	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
374	Th1162	Register an ineligible person	Register as an unregistered but ineligible person (e.g., non-citizens, felons)	Election system: lack of records management	human-deliberate	malicious outsider(s)	strengthen the controls in the ElectionSystem	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
375	Th1163	Register as a dead person	Register as a deceased or incapacitated person	Election system: lack of records management	human-deliberate	malicious outsider(s)	strengthen the controls in the ElectionSystem	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
376	Th1165	Based on legalvoter lists	Make lists of voters very unlikely to vote this election or likely to vote late in the day	Voter registration databases: access to voter lists and ability to determine voters not likely to vote	human-deliberate	malicious outsider(s)	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
377	Th1166	Based on fraudulent registrations	Create fraudulent voter registrations	Election system: poor vetting process, lack of resources, legal constraints on voter registration process	human-deliberate	malicious outsider(s)	strengthen the controls in the ElectionSystem	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.

Index ID	Source ID	Threat Vector	Threat Event	Vulnerability	Threat Agent Category	Threat Agent(s)	Potential Mitigation	Source	Reference
378	Th1167	Execute impersonated voting	Execute impersonated voting	Authenticate voter: failure of election day administration to foil attack	human-deliberate	malicious outsider(s)	physical and environmental protection, audit and accountability, identification and authentication	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
379	Th1168	Voters likely to vote late in the day	Make lists of voters likely to vote late in the day	Voter lists: access to voter lists and ability to identify target voters	human-deliberate	malicious outsider(s)	chain of custody controls on voter registration lists, if not public information	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
380	Th1169	Supply rewards or punishment	Provide promised rewards or punishments based on voter compliance	Post certification audit: difficulty in tracing payments	human-deliberate	malicious outsider(s)	personnel security, including sanctions against violators	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
381	Th1170	Direct voter	Direct voter to make specific votes according to attacker's demands	Folded marked ballot,: corrupt poll worker or voter who can easily be intimidated; poll workers and poll observers unable to detect concealed ballots	human-deliberate	malicious outsider(s)	1.Ballot Distribution Security 2. Mark absentee ballots distinctly to distinguish them from ballots voted. 3.Prevent Ballot Counterfeiting. 4.Serial Number Ballots	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
382	Th1171	Punish and promise more	Provide a real punishment, and then promise more punishment of not compliant	Eligible voter, signed in voter: susceptibility of voters to intimidation; lack of voter privacy	human-deliberate	malicious outsider(s)	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and poll workers	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
383	Th1172	Punish and promise repair	Provide a real punishment, and then promise a repair of punishment	Eligible voter, signed in voter: susceptibility of voters to intimidation; lack of voter privacy	human-deliberate	malicious outsider(s)	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and poll workers	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
384	Th1174	Conceal poll book tampering	Conceal poll book tampering to reduce the risk of detection	Poll book: lack of access controls on poll book	human-deliberate	malicious insider(s)	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
385	Th1175	Wait until polls close	Wait until polls close to tamper with poll book	Poll book: lack of access controls on poll book	human-deliberate	malicious insider(s)	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
386	Th1176	Make excuses for marked poll book	Make excuses in case voters show up, and the poll book is pre-signed	Election official: difficulty in determining the truth when poll workers are lying	human-deliberate	malicious insider(s)	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
387	Th1177	Mark votableballot	Mark votableballot	Voter: inability to verify voters vote due to lack of voter attribution	human-deliberate	malicious insider(s)	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
388	Th1178	Obtain votableballot	Obtain votableballot	One voter: poll worker discretion to instruct voter; voter's lack of understanding	human-deliberate	malicious insider(s)	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
389	Th1179	Subvert markedballot of voter	Subvert markedballot of checkedin voter at polls	Voter, marked ballot: inability to verify vote with voter, lack of management oversight	human-deliberate	malicious insider(s)	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
390	Th1180	Mark undervote to create vote	Mark undervote to create vote	Voter: inability to verify voters vote due to lack of voter attribution	human-deliberate	malicious insider(s)	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
391	Th1181	Mark vote to create overvote	Mark vote to create overvote	Voter: inability to verify voters vote due to lack of voter attribution	human-deliberate	malicious insider(s)	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
392	Th1182	Swap ballot with new markedballot	Swap ballot with new markedballot	Marked ballot: lack of management oversight	human-deliberate	malicious insider(s)	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
393	Th1186	Persuade or coerce	Coerce the voter to vote for the attacker's candidate(s)	Voters: human susceptibility to being coerced	human-deliberate	malicious outsider(s)	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and poll workers	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
394	Th1189	Replace ballots	Switch legitimate ballots with tampered ballots	Ballots: access to ballots; lack of management oversight	human-deliberate	malicious insider(s)	establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
395	Th1190	Switch valid ballots with tampered ones	Switch a set of valid ballots with the ones the tampered ballots	Ballots: access to ballots; lack of management oversight	human-deliberate	malicious insider(s)	establish ballot chain of custody procedures, including ballot distribution security, physical and other access controls on ballots, anti-counterfeit measures, serial ballot numbering, and personnel policies related to access; auditing and accountability procedures	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
396	Th1192	Issue erroneous votableballot of the incorrect ballot style	Issue an incorrect ballot style, that is, a ballot for a different precinct	Voter: possibility that voter will not catch error	human-unintentional	local election official	poll worker awareness and training	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
397	Th1193	Issue erroneous votableballot with errors in contests or candidates	Issue ballot with mistakes in the contests or candidates	Voter: possibility that voter will not catch error	human-unintentional	local election official	pre-election ballot validation	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
398	Th1194	Mishandle ballots	Mishandle ballots	Ballots: poor planning	human-unintentional	local election official	physical and environmental protection, media protection policy and procedures, personnel security, awareness and training, ballot accounting / reconciliation	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
399	Th1195	With errors in selection rules	Issue ballots with errors in selection rules	Voter: possibility that voter will not catch error	human-deliberate	malicious insider(s)	pre-election ballot validation	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.

Index ID	Source ID	Threat Vector	Threat Event	Vulnerability	Threat Agent Category	Threat Agent(s)	Potential Mitigation	Source	Reference
400	Th1196	By misapplying rules for determining voter intent	Misapply the rules for interpreting the intent of the voter	Accumulation, retabulation, reconcile voter feedback: unclear rules of behavior or failure to follow rules, human error	human-deliberate	malicious insider(s)	clearly defined counting rules, poll worker training, multi-person integrity check	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Saltman, R. G. (2006).The history and politics of voting technology: In quest of integrity and public confidence. New York: Palgrave Macmillan. Jones, Doug W. (2002) "Counting Mark-Sense Ballots: Relating Technology, the Law and common Sense," The Voting and Elections web pages, University of Iowa, 2002, Retrieved from http://www.cs.uiowa.edu/~jones/voting/optical/
401	Th1197	By making counting mistakes	Make counting mistakes when accumulating totals by hand	Accumulation, retabulation, reconcile voter feedback: fatigue, unclear counting rules, misinterpret counting rules	human-deliberate	malicious insider(s)	start counting well before polls close; use dedicated counting team; have new hires work under trainers; take breaks after each hour of counting; use techniques not prone to error; checking	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
402	Th1198	Incorrectly accept ballots	Incorrectly accept ballots with non-legal marks	Validate precinct results, resolve provisional ballots, reconcile voter feedback: fallibility of human judgment; misinterpretation of rules	human-deliberate	malicious insider(s)	poll worker training, clear rules for ballot adjudication, transparent processes, personnel sanctions	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
403	Th1199	By losing a batch of ballots	By losing a batch of ballots	Accumulation, retabulation, reconcile voter feedback: fatigue, human error, lack of oversight	human-deliberate	malicious insider(s)	ballot accounting, chain of custody, personnel sanctions	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
404	Th1200	By mislabeling a batch of ballots	By mislabeling a batch of ballots	Accumulation, retabulation, reconcile voter feedback: fatigue, human error, lack of oversight	human-deliberate	malicious insider(s)	ballot accounting, chain of custody, personnel sanctions	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
405	Th1201	Based on candidate	Inconsistently apply rules for determining voter intent based for different candidates	Contest results, candidate, political parties: lack of transparency, poor verification process	human-deliberate	malicious insider(s)	election law, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
406	Th1202	Based on polling place	Inconsistently apply rules for determining voter intent, depending on which polling place	Contest results, candidate, political parties: lack of transparency, poor verification process	human-deliberate	malicious insider(s)	election law, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
407	Th1203	Subvert counting process	Subvert counting process	Contest results: poor counting and verification processes, lack of transparency	human-deliberate	malicious insider(s)	election law, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
408	Th1204	By intentionally miscounting	Subvert counting process by intentionally miscounting	Contest results: poor counting and verification processes, lack of transparency	human-deliberate	malicious insider(s)	election law, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
409	Th1205	By subverting straight-party vote	Subvert counting process by subverting straight-party vote	Contest results: poor counting and verification processes, lack of transparency	human-deliberate	malicious insider(s)	election law, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
410	Th1210	Subvert validation process	Subvert validation process	Ballotboxaccounting, validate precinct results, validate jurisdiction results: lack of transparency, poor verification process	human-deliberate	malicious insider(s)	election law, awareness and training, transparent processes, multi-person, multi-party controls, audit and accountability	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
411	Th1211	By subverting ballot adjudication	Subvert counting process by subverting ballot adjudication	Contest results: dependence on key election official(s) with centralized power to announce / certify result	human-deliberate	malicious insider(s)	planning: establish clear and effective rules for ballot adjudication; personnel security: implement personnel sanctions; awareness and training	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
412	Th1216	Experience a fire	Experience a fire that affects the availability of or effective operation of the polling place	Polling places: exposure to natural or accidental events	accidental	environmental	All electrical wiring and equipment should be thoroughly checked. Restrict smoking and presence of flammable materials in the polling place	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Potts, Ted (2008) "Fire Guts Patton Store, Forces Change of Polls," The Tribune Democrat, November 5, 2008, Retrieved from http://www.tribune-democrat.com/local/local_story_310012455.html
413	Th1217	Experience power disruptions	Experience unintended power disruptions	Rooms needing lighting: lack of control over utility providers	accidental	environmental	contingency planning, incident response	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
414	Th1218	Experience effects of humidity	Experience effects of humidity on ballots, including ink bleeding	Votable ballots, marked ballots: exposure to humid environments	accidental	natural	Marked ballots that have been stored in a high humidity (>90%) environment, and with ink that tends to bleed, are retrieved for recounting, and result in a different result because of bleeding being reinterpreted as stray marks	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
415	Th1219	Run out of ballots	Run out of votable ballot stock	Votable ballot stock: poor planning; process whereby ballots must be preprinted	human-unintentional	local election official	plan well and print plenty of ballots; fewer ballot styles; ballot on demand	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
416	Th1220	Issue incorrect ballot style	Issue voter an incorrect ballot style	Voter: possibility that threat will go undetected by voter	human-deliberate	malicious insider(s)	personnel security, voter education	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
417	Th1221	That exploit leaked results	Target polling places that exploit leaked partial results of hand count before the polls close	Election artifacts: difficulty controlling insiders with knowledge of partial results	human-deliberate	malicious insider(s)	implement personnel policies and sanctions to prevent disclosure; monitor personnel doing the recount	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
418	Th1222	Due to language differences	Due to language differences	Poll worker: lack of multilingual skills among poll workers, unclear language requirements	human-unintentional	voter; local election official	clarify language requirements; employ poll workers with multilingual skills; use single multilingual rather than separate ballots	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
419	Tm1231	Edit marked ballots	Make, or delete, a mark on a marked ballot.	Marked ballot: insider's access to ballots	human-deliberate	malicious insider(s)	None provided in reference.	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
420	Tm1232	Edit at local elections office	Edit during one of the vbm processing steps at the leo	Marked ballot: insider's access to ballots	human-deliberate	malicious insider(s)	None provided in reference.	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.

Index ID	Source ID	Threat Vector	Threat Event	Vulnerability	Threat Agent Category	Threat Agent(s)	Potential Mitigation	Source	Reference
421	Tm1233	Edit during duplication	Edit during the vbm ballots duplication process at the leo.	Marked ballot: insider's access to ballots	human-deliberate	malicious insider(s)	(1) Two person integrity (2) Require independent oversight (3) Videotape duplication process (4) PW whistleblower program	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
422	Tm1237	Mark under/overvotes or change votes	Make selections in races that were not marked, or in races that were marked to create an overvote, or change votes if possible.	Marked ballot: access to ballots; inability to bind marked ballot to voter	human-deliberate	malicious insider(s)	(1) Two person integrity (2) Require independent oversight (3) Videotape duplication process (4) PW whistleblower program	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
423	Tm1238	Edit during counting	Edit vbm ballots during the counting process at the leo	Marked ballot: poor oversight, lack of transparency of counting process	human-deliberate	malicious insider(s)	(1) Two person integrity (2) Require independent oversight (3) Videotape counting process (4) PW whistleblower program	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
424	Tm1239	Edit during other handling	Edit vbm ballots during other handling processes that are unique to vbm ballots at the leo	Marked ballot: lack of transparency, oversight; broken chain of ballot custody	human-deliberate	malicious insider(s)	(1) Two person integrity (2) Require independent oversight (3) Videotape handling process	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
425	Tm1240	Edit in transit	Edit vbm ballots in the mail or other delivery process.	Marked ballot, envelope: lack of physical protection/control of ballots	human-deliberate	malicious insider(s)	(1) Tamper-resistant envelopes (2) Legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	NIST Andrew Regenscheid and Nelson Hastings, A Threat Analysis on UOCAVA Voting Systems. NISTIR 7551, December 2008, Retrieved from http://vote.nist.gov/uocava-threatanalysis-final.pdf
426	Tm1241	Edit in post office	Edit vbm ballots at a post office where the ballot passes in transit from the voter to the leo.	Marked ballot, envelope: lack of physical protection/control of ballots	human-deliberate	malicious insider(s)	(1) Tamper-resistant envelopes (2) Two person integrity for envelopes at the post office	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	NIST Andrew Regenscheid and Nelson Hastings, A Threat Analysis on UOCAVA Voting Systems. NISTIR 7551, December 2008, Retrieved from http://vote.nist.gov/uocava-threatanalysis-final.pdf
427	Tm1242	Edit in intermediate mail room	Edit vbm ballots at an intermediate mail room where the ballot passes in transit from the voter to the leo.	Marked ballot, envelope: lack of physical protection/control of ballots	human-deliberate	malicious insider(s)	(1) Tamper-resistant envelopes	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	NIST Andrew Regenscheid and Nelson Hastings, A Threat Analysis on UOCAVA Voting Systems. NISTIR 7551, December 2008, Retrieved from http://vote.nist.gov/uocava-threatanalysis-final.pdf
428	Tm1243	Discard marked ballot	Steal, destroy, or otherwise preclude vbm ballots from tabulation.	Marked ballot: faulty validation process; personnel training or integrity issues; delivery failures	human-deliberate	malicious insider(s)	(1) Rigorous audit procedures for detection/deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
429	Tm1244	Challenge committed ballot	Challenge a vbm ballot in order to prevent its tabulation	Validate remote ballot: faulty validation process	human-deliberate	malicious insider(s)	None provided in reference.	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
430	Tm1246	Judge misinterprets rule	A judge challenges a vbm ballot in error because she misunderstands a rule	Validate remote ballot: faulty validation process	human-unintentional	local election official	(1) Clear challenge rules (2) Challenge rule training (3) Responsive escalation process	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
431	Tm1247	Errant failed signature	A signature judge wrongly adjudicates that a ballot signature does not match the registration signature and prevents the ballot from being tabulated.	Validate remote ballot: faulty validation process; poorly trained election officials	human-unintentional	local election official	(1) Signature recognition training (2) Two person signature verification integrity (3) Escalation process for signature rejection	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
432	Tm1248	Malicious challenge	An attempt to prevent ballot tabulation by claiming that the voter/ballot violates an elections rule.	Validate remote ballot: lack of integrity of election official	human-deliberate	malicious insider(s)	(1) Legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
433	Tm1249	Challenge signature	Challenge a ballot because the voter's signature does not match the registration signature.	Validate remote ballot: lack of integrity of election official	human-deliberate; human-unintentional	malicious insider(s); local election official	(1) Two person signature verification integrity (2) Escalation process for signature rejection	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
434	Tm1250	Challenge postmark	Challenge a ballot because the postmark date does not satisfy the date requirement for the election.	Validate remote ballot: lack of integrity of election official	human-deliberate	malicious insider(s)	(1) Two person postmark verification integrity (2) Escalation process for postmark rejection	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
435	Tm1251	Challenge intent	Challenge a ballot because one or more marks do not satisfy the published mark standard.	Validate remote ballot: lack of integrity of election official	human-deliberate	malicious insider(s)	(1) Use machine marking (2) Use marking template (3) Ignore unofficial marks	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
436	Tm1252	Marked ballot lost in the mail	A vbm ballot is destroyed or misplaced in the mail system.	Marked ballot: lack of control over delivery process; inability to recover lost ballots	human-deliberate; human-unintentional	malicious insider(s); mail employee; ISP technician	(1) Dual submit electronically (2) Utilize an independent tracking process. (3) Receipt-based courier	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Hackett, Alexandra, "Clearwater post office loses 1100 absentee ballots", 10Connects.com, March 15, 2008, Retrieved from http://www.tampabays10.com/includes/tools/print.aspx?storyid=76237.
437	Tm1253	Malicious loss	A vbm ballot is intentionally destroyed or misplaced in the mail system.	Marked ballot: lack of control over delivery process; inability to recover lost ballots	human-deliberate	malicious insider(s)	(1) Dual submit electronically (2) Utilize an independent tracking process. (3) Receipt-based courier with chain of custody	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	NIST Andrew Regenscheid and Nelson Hastings, A Threat Analysis on UOCAVA Voting Systems. NISTIR 7551, December 2008, Retrieved from http://vote.nist.gov/uocava-threatanalysis-final.pdf
438	Tm1254	Accidental loss	A vbm ballot is unintentionally destroyed or misplaced in the mail system.	Marked ballot: lack of control over delivery process; inability to recover lost ballots	human-unintentional	mail employee; ISP technician	(1) Dual submit electronically (2) Utilize an independent tracking process. (3) Receipt-based courier with chain of custody	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	NIST Andrew Regenscheid and Nelson Hastings, A Threat Analysis on UOCAVA Voting Systems. NISTIR 7551, December 2008, Retrieved from http://vote.nist.gov/uocava-threatanalysis-final.pdf
439	Tm1255	Discard marked ballots at leo	A marked ballot is lost, destroyed, or disposed of at the leo.	Marked ballot: insider's access to ballots	human-deliberate	malicious insider(s)	(1) Two person integrity (2) Use rigorous chain of custody protection	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
440	Tm1256	Delete during duplication	A marked ballot is destroyed or disposed of during the ballot duplication process.	Marked ballot: insider's access to ballots	human-deliberate	malicious insider(s)	(1) Two person integrity (2) Use rigorous chain of custody protection (3) Require independent oversight (3) video tape duplication	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Yasinsac, A. and Bishop. M. (2008). The Dynamics of Counting and Recounting Votes.IEEE S&P Magazine, 6(3), 22-29. Yasinsac, A. and Bishop, M. (2008). Of Paper Trails and Voter Receipts.Proceedings of the 41st Hawaii International Conference on System Sciences.
441	Tm1257	Form collaboration of pws	Form an alliance of pws that will collude to edit ballots at the leo.	Poll worker: susceptibility to bribery and coercion	human-deliberate	malicious insider(s)	(1) Background check (2) Require worker-signed "honesty statement".	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
442	Tm1258	Gain exclusive access to ballots	Isolate ballots so that only colluding pws are able to observe vbm ballots at the leo.	Marked ballot: gaps in the chain of ballot custody procedures	human-deliberate	malicious insider(s)	(1) Two-person integrity rules (2) Rigorous protection procedures/facilities for marked ballots.	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
443	Tm1260	Remove during counting	Remove ballots during the counting process at the leo	Marked ballot: poor oversight, lack of transparency of counting process	human-deliberate	malicious insider(s)	(1) Chain of custody (2) Two person integrity (3) Rigorous oversight	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
444	Tm1261	Remove during other handling	Remove ballots during other handling processes at the leo	Marked ballot: lack of transparency, oversight; broken chain of ballot custody	human-deliberate	malicious insider(s)	(1) Chain of custody (2) Two person integrity (3) Rigorous oversight	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Yasinsac, A. and Bishop. M. (2008). The Dynamics of Counting and Recounting Votes.IEEE S&P Magazine, 6(3), 22-29. Yasinsac, A. and Bishop, M. (2008). Of Paper Trails and Voter Receipts.Proceedings of the 41st Hawaii International Conference on System Sciences.
445	Tm1262	Miscount duplicated ballots	Cause duplicated ballots to be incorrectly tabulated.	Precinct data: lack of transparency, oversight	human-deliberate	malicious insider(s)	(1) Two person integrity (2) Require independent oversight (3) Videotape counting process	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.

Index ID	Source ID	Threat Vector	Threat Event	Vulnerability	Threat Agent Category	Threat Agent(s)	Potential Mitigation	Source	Reference
446	Tm1263	Count original & duplicate	Cause both duplicate and duplicated ballots to be tabulated.	Precinct data: lack of transparency, oversight	human-deliberate	malicious insider(s)	(1) Two person integrity (2) Require independent oversight (3) Videotape counting process (4) Audit via ballot accounting	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Yasinsac, A. and Bishop. M. (2008). The Dynamics of Counting and Recounting Votes.IEEE S&P Magazine, 6(3), 22-29. Yasinsac, A. and Bishop, M. (2008). Of Paper Trails and Voter Receipts.Proceedings of the 41st Hawaii International Conference on System Sciences.
447	Tm1264	File duplicate with duplicated ballot	Cause both duplicate and duplicated ballots to be stored as counted ballots.	Precinct data: lack of transparency, oversight	human-deliberate	malicious insider(s)	(1) Two person integrity (2) Require independent oversight (3) Videotape counting process (4) Audit via ballot accounting	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Yasinsac, A. and Bishop. M. (2008). The Dynamics of Counting and Recounting Votes.IEEE S&P Magazine, 6(3), 22-29. Yasinsac, A. and Bishop, M. (2008). Of Paper Trails and Voter Receipts.Proceedings of the 41st Hawaii International Conference on System Sciences.
448	Tm1265	Defeat ballot accounting	Cause confusion or inconsistencies in ballot accounting procedures.	Precinct data: lack of transparency, oversight	human-deliberate	malicious insider(s)	(1) Two person integrity (2) Require independent oversight (3) Videotape counting process	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
449	Tm1266	Omit original & duplicate	Cause both duplicate and duplicated ballots to be stored as spoiled ballots.	Duplicated ballot, duplicate ballot: lack of transparency, oversight; inability to detect or recover	human-deliberate	malicious insider(s)	(1) Two person integrity (2) Require independent oversight (3) Videotape counting process (4) Audit via ballot accounting	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
450	Tm1267	Marked ballot stuffing	Insert illegitimate ballots into tabulation.	Precinct data: lack of transparency, oversight; inability to detect or recover	human-deliberate	malicious insider(s)	(1) Two person integrity (2) Require independent oversight (3) Audit via ballot accounting	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Sherman, Ted, "Fifth person charged with voter fraud in 2007 N.J. Senate election", The Star-Ledger, August 18, 2009, Retrieved from http://www.nj.com/news/index.ssf/2009/08/fifth_person_indicted_for_vote.html
451	Tm1268	Insert ballots during envelope separation	During envelope separation, workers may be able to insert pre-marked ballots into tabulation unnoticed.	Precinct data: lack of transparency, oversight; inability to detect or recover	human-deliberate	malicious insider(s)	(1) Two person integrity (2) Require independent oversight (3) Videotape ballot opening (4) Audit via ballot accounting	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
452	Tm1269	Insert ballots during counting	During vbm counting, workers may be able to insert pre-marked ballots into tabulation unnoticed.	Precinct data: lack of transparency, oversight; inability to detect or recover	human-deliberate	malicious insider(s)	(1) Two person integrity (2) Require independent oversight (3) Videotape ballot opening (4) Audit via ballot accounting	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
453	Tm1270	Insert ballots during recount	During a recount, workers may be able to insert pre-marked ballots into tabulation unnoticed.	Jurisdiction results: lack of transparency, oversight; inability to detect or recover	human-deliberate	malicious insider(s)	(1) Two person integrity (2) Require independent oversight (3) Videotape ballot opening (4) Audit via ballot accounting	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
454	Tm1271	Insert ballots during audit	During an audit workers may be able to insert pre-marked ballots into tabulation unnoticed.	Audit results: lack of transparency, oversight; inability to detect or recover	human-deliberate	malicious insider(s)	(1) Two person integrity (2) Require independent oversight (3) Videotape ballot opening (4) Audit via ballot accounting	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
455	Tm1272	Manipulate or discard votable ballot	Prevent distribution of a votable ballot to a valid vbm voter.	Votable ballot: faulty validation process; personnel training or integrity issues; delivery failures	human-deliberate	malicious insider(s)	(1) Two person integrity (2) Require independent oversight (3) Videotape envelop preparation	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Hackett, Alexandra, "Clearwater post office loses 1100 absentee ballots", 10Connects.com, March 15, 2008, Retrieved from http://www.tampabays10.com/includes/tools/print.aspx?storyid=76237.
456	Tm1273	Delete at leo	Take action at the leo that prevents a votable ballot from being distributed to a legitimate vbm voter.	Votable ballot: faulty validation process; personnel training or integrity issues; delivery failures	human-deliberate	malicious insider(s)	(1) Two person integrity (2) Require independent oversight (3) Videotape envelop preparation	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
457	Tm1274	Fail to stuff envelope	During vbm envelope preparation, prepare an envelope for mailing without inserting a votable ballot.	Votable ballot: faulty validation process; personnel training or integrity issues; delivery failures	human-deliberate	malicious insider(s)	(1) Two person integrity (2) Require independent oversight (3) Videotape envelop preparation	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
458	Tm1275	Send wrong or premarked ballot	During vbm envelope preparation, prepare an envelope for mailing with a votable ballot that for other than the voter's precinct.	Votable ballot: faulty validation process; personnel training or integrity issues; delivery failures	human-deliberate	malicious insider(s)	(1) Two person integrity (2) Require independent oversight (3) Videotape envelop preparation	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
459	Tm1276	Mis-address envelope	During vbm envelope preparation, prepare an envelope for mailing with an errant address.	Votable ballot: faulty validation process; personnel training or integrity issues	human-deliberate	malicious insider(s)	(1) Two person integrity (2) Require independent oversight (3) Videotape envelop preparation	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
460	Tm1277	Destroy prepared envelope	During vbm envelope preparation, destroy or dispose of a previously prepared envelope.	Votable ballot: faulty validation process; personnel training or integrity issues	human-deliberate	malicious insider(s)	(1) Two person integrity (2) Require independent oversight (3) Videotape envelop preparation (4) Chain of custody	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
461	Tm1278	Destroy batch of prepared envelopes	During vbm envelope preparation, destroy or dispose of a batch of previously prepared envelopes.	Votable ballot: faulty validation process; personnel training or integrity issues	human-deliberate	malicious insider(s)	(1) Two person integrity (2) Require independent oversight (3) Chain of custody	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
462	Tm1279	Delay delivery past deadline	Delay delivery of prepared vbm envelopes to the post office.	Votable ballot: personnel training or integrity issues; delivery failures	human-deliberate	malicious insider(s)	(1) Registered mail	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
463	Tm1280	Election process delay	Cause election events that delay vbm ballot preparation.	Votable ballot: personnel training or integrity issues; delivery failures	human-deliberate	malicious insider(s)	(1) Registered mail	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
464	Tm1281	Handling delay	vbm ballot handling problem that delays envelope delivery.	Votable ballot: personnel training or integrity issues; delivery failures	human-deliberate; human-unintentional	malicious insider(s); mail employee; ISP technician	(1) Registered mail	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Pew: No Time to Vote, Challenges Facing Americas Overseas and Military Voters. January 2009, http://www.pewtrusts.org/uploadedFiles/wwwpewtrustsorg/Reports/Election_reform/NTTV_Report_Web.pdf
465	Tm1282	Delay in the mail	Mail event that delays delivery of prepared vbm envelopes to valid voters.	Votable ballot: personnel training or integrity issues; delivery failures	equipment failure; human-deliberate	hardware; software; malicious outsider(s)	(1) Registered mail	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Pew: No Time to Vote, Challenges Facing Americas Overseas and Military Voters. January 2009, http://www.pewtrusts.org/uploadedFiles/wwwpewtrustsorg/Reports/Election_reform/NTTV_Report_Web.pdf
466	Tm1283	Delete at destination	Delete or destroy vbm ballots after they reach their postal destination.	Votable ballot: personnel training or integrity issues; delivery failures	human-deliberate	malicious insider(s)	(1) Remote ballot status process	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	NIST Andrew Regenscheid and Nelson Hastings, A Threat Analysis on UOCAVA Voting Systems. NISTIR 7551, December 2008, Retrieved from http://vote.nist.gov/uocava-threatanalysis-final.pdf
467	Tm1284	Lost in destination mail room	Vbm ballot/envelope misplaced or destroyed at an intermediate mail room after deliver from the postal system.	Votable ballot: personnel training or integrity issues; delivery failures	human-deliberate; human-unintentional	malicious insider(s); mail employee; ISP technician	(1) Remote ballot status process	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	NIST Andrew Regenscheid and Nelson Hastings, A Threat Analysis on UOCAVA Voting Systems. NISTIR 7551, December 2008, Retrieved from http://vote.nist.gov/uocava-threatanalysis-final.pdf
468	Tm1285	Mail box attack	Remove vbm ballot/ envelope from the voter's mailbox.	Votable ballot: personnel training or integrity issues; delivery failures	human-deliberate	malicious outsider(s)	(1) Remote ballot status process (2) Strong ballot fraud legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	NIST Andrew Regenscheid and Nelson Hastings, A Threat Analysis on UOCAVA Voting Systems. NISTIR 7551, December 2008, Retrieved from http://vote.nist.gov/uocava-threatanalysis-final.pdf
469	Tm1286	Masquerade attack	Vote for a legitimate voter other than yourself.	Eligible voter: personnel training or integrity issues; faulty authentication	human-deliberate	malicious outsider(s)	(1) Strong vote attribution procedures	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Sherman, Ted, "Fifth person charged with voter fraud in 2007 N.J. Senate election", The Star-Ledger, August 18, 2009, Retrieved from http://www.nj.com/news/index.ssf/2009/08/fifth_person_indicted_for_vote.html

Index ID	Source ID	Threat Vector	Threat Event	Vulnerability	Threat Agent Category	Threat Agent(s)	Potential Mitigation	Source	Reference
470	Tm1287	Deceased voters	Cast a vbm ballot using a deceased voter's identity.	Eligible voter: personnel training or integrity issues; faulty authentication	human-deliberate	malicious outsider(s)	(1) Accurate voter rolls (2) Strong vote attribution procedures	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Estep, Bill, "Clay Co. vote-buying investigation keeps expanding" Lexington Herald-Leader, Monday, May. 18, 2009 http://www.kentucky.com/181/story/799167.html
471	Tm1288	Identify target deceased voters	Match voter rolls against online obituary entries or identify deceased voters for whom they can register.	Eligible voter: personnel training or integrity issues; faulty authentication	human-deliberate	malicious outsider(s)	(1) Accurate voter rolls	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
472	Tm1289	Register them to an accessible address	Register the identified deceased voter to an address where the attacker can easily retrieve the delivered vbm votable ballot.	Eligible voter: personnel training or integrity issues; faulty authentication	human-deliberate	malicious outsider(s)	(1) Strong voter authentication	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
473	Tm1291	Defeat signature check	The primary mechanism used to verify identity is a signature check. overcoming that control allows successful masquerade.	Eligible voter: personnel training or integrity issues; faulty authentication	human-deliberate	malicious outsider(s)	(1) Signature match training	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
474	Tm1292	Family members	Cast a vbm ballot using a family member's identity or alter a family member's ballot.	Eligible voter: personnel training or integrity issues; faulty authentication	human-deliberate	malicious outsider(s)	(1) Strong vote attribution procedures	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
475	Tm1293	Central housing	Cast a vbm ballot using a cohabitant of a central housing facility's identity.	Eligible voter: personnel training or integrity issues; faulty authentication	human-deliberate	malicious outsider(s)	(1) Strong vote attribution procedures	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Sherman, Ted, "Fifth person charged with voter fraud in 2007 N.J. Senate election", The Star-Ledger, August 18, 2009, Retrieved from http://www.nj.com/news/index.ssf/2009/08/fifth_person_indicted_for_vote.html
476	Tm1294	Identify target residents	Identify residents that are legitimate voters that are unlikely to vote, and from whom you can acquire their vbm materials.	Eligible voter: personnel training or integrity issues; faulty authentication	human-deliberate	malicious outsider(s)	(1) Strong legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Sherman, Ted, "Fifth person charged with voter fraud in 2007 N.J. Senate election", The Star-Ledger, August 18, 2009, Retrieved from http://www.nj.com/news/index.ssf/2009/08/fifth_person_indicted_for_vote.html
477	Tm1295	Register them	Represent yourself as a cohabiting voter by filing registration forms in their name.	Eligible voter: personnel training or integrity issues; faulty authentication	human-deliberate	malicious outsider(s)	(1) Strong voter authentication	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Sherman, Ted, "Fifth person charged with voter fraud in 2007 N.J. Senate election", The Star-Ledger, August 18, 2009, Retrieved from http://www.nj.com/news/index.ssf/2009/08/fifth_person_indicted_for_vote.html
478	Tm1296	Intercept, mark, and return their ballot	Intercept, mark, and return their ballot	Eligible voter: personnel training or integrity issues; faulty authentication	human-deliberate	malicious outsider(s)	(1) Strong vote attribution procedures	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Yasinsac, A. and Bishop. M. (2008). The Dynamics of Counting and Recounting Votes.IEEE S&P Magazine, 6(3), 22-29. Yasinsac, A. and Bishop, M. (2008). Of Paper Trails and Voter Receipts.Proceedings of the 41st Hawaii International Conference on System Sciences.
479	Tm1299	Forge the signature	Forge the signature	Eligible voter: personnel training or integrity issues; faulty authentication	human-deliberate	malicious outsider(s)	(1) Strong voter authentication, (2) Signature match training	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Yasinsac, A. and Bishop. M. (2008). The Dynamics of Counting and Recounting Votes.IEEE S&P Magazine, 6(3), 22-29. Yasinsac, A. and Bishop, M. (2008). Of Paper Trails and Voter Receipts.Proceedings of the 41st Hawaii International Conference on System Sciences.
480	Tm1302	Steal blank ballot from mailbox	Steal blank ballot from mailbox	Eligible voter: personnel training or integrity issues; faulty authentication	human-deliberate	malicious outsider(s)	(1) Strong legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Yasinsac, A. and Bishop. M. (2008). The Dynamics of Counting and Recounting Votes.IEEE S&P Magazine, 6(3), 22-29. Yasinsac, A. and Bishop, M. (2008). Of Paper Trails and Voter Receipts.Proceedings of the 41st Hawaii International Conference on System Sciences.
481	Tm1308	Internet vote buying attack	Attacker uses Internet capabilities to reach masses and to overcome legal deterrence.	Remote voter: susceptibility to bribery and coercion	human-deliberate	malicious outsider(s)	(1) Strong vote attribution (2) Receipt-free voting process (3) Strong legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
482	Tm1309	Attract voters	Vote buyers must find eligible voters that are willing to sell their vote.	Remote voter: susceptibility to bribery and coercion	human-deliberate	malicious outsider(s)	(1) Strong legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Estep, Bill, "Clay Co. vote-buying investigation keeps expanding" Lexington Herald-Leader, Monday, May. 18, 2009 http://www.kentucky.com/181/story/799167.html
483	Tm1311	Pay the voters via the Internet	Voters may be paid via any of several Internet payment companies.	Remote voter: susceptibility to bribery and coercion	human-deliberate	malicious outsider(s)	(1) Strong legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
484	Tm1312	Organizer coercion attack	An organizer may be a government organization or public group.	Remote voter: susceptibility to bribery and coercion	human-deliberate	malicious outsider(s)	(1) Strong vote attribution (2) Receipt-free voting process (3) Strong legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Hester, Tom Sr, "Roselle council president charged with illegally filling out absentee ballots", August 27, 2009, Retrieved from http://www.nj.gov/oag/newsreleases09/pr20090827b.html
485	Tm1313	Attribution threats	An organizer may intimidate voters by claiming that they can identify voter selections.	Remote voter: susceptibility to bribery and coercion	human-deliberate	malicious outsider(s)	(1) Receipt-free voting process (2) Strong legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
486	Tm1314	Debate and vote parties	Groups may encourage members to bring their blank vbm ballots to "parties" and apply peer pressure to influence their selections.	Remote voter: susceptibility to bribery and coercion	human-deliberate	malicious outsider(s)	(1) Receipt-free voting process (2) Strong legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Johnson, Kirk (2009) "Rise in Voting by Mail Transforms Race in Colorado", August 27, 2009, Retrieved from http://www.nytimes.com/2008/10/17/us/politics/17colorado.html
487	Tm1315	Employer coercion attack	Employer coercion attack	Remote voter: susceptibility to bribery and coercion	human-deliberate	malicious outsider(s)	(1) Receipt-free voting process (2) Strong legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
488	Tm1317	Administrative error	Many vbm ballots are disqualified for administrative errors, preventing otherwise legitimate vbm ballots from being tabulated.	Remote voter: faulty validation process; poorly trained election officials	human-unintentional	local election official	(1) Clear rules (2) Simple procedures (3) Explicit instructions	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Yasinsac, A. and Bishop. M. (2008). The Dynamics of Counting and Recounting Votes.IEEE S&P Magazine, 6(3), 22-29. Yasinsac, A. and Bishop, M. (2008). Of Paper Trails and Voter Receipts.Proceedings of the 41st Hawaii International Conference on System Sciences.
489	Tm1318	Failure to sign correctly	Since signature matching is the primary vbm authentication method, rules may be precisely enforced, so even minor deviations may disqualify an otherwise legitimate vbm ballot.	Remote voter: faulty validation process; poorly trained election officials	human-unintentional	local election official	(1) Clear rules (2) Simple procedures (3) Explicit instructions	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Yasinsac, A. and Bishop. M. (2008). The Dynamics of Counting and Recounting Votes.IEEE S&P Magazine, 6(3), 22-29. Yasinsac, A. and Bishop, M. (2008). Of Paper Trails and Voter Receipts.Proceedings of the 41st Hawaii International Conference on System Sciences.
490	Tm1319	Signature mismatch	Signature deviations and errors by officials can cause erroneous mismatch disqualifications that prevent legitimate vbm ballots from being tabulated.	Remote voter: faulty validation process; poorly trained election officials	human-unintentional	local election official	(1) Signature match training (2) Signature mis-match escalation procedure	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Yasinsac, A. and Bishop. M. (2008). The Dynamics of Counting and Recounting Votes.IEEE S&P Magazine, 6(3), 22-29. Yasinsac, A. and Bishop, M. (2008). Of Paper Trails and Voter Receipts.Proceedings of the 41st Hawaii International Conference on System Sciences.
491	Tm1320	Failure to bundle correctly	Instructions for what must be returned and how it must be packaged may be confusing and may be precisely enforced, preventing otherwise legitimate vbm ballots from being tabulated.	Remote voter: faulty validation process; poorly trained election officials	human-unintentional	local election official	(1) Clear rules (2) Simple procedures (3) Explicit instructions	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Yasinsac, A. and Bishop. M. (2008). The Dynamics of Counting and Recounting Votes.IEEE S&P Magazine, 6(3), 22-29. Yasinsac, A. and Bishop, M. (2008). Of Paper Trails and Voter Receipts.Proceedings of the 41st Hawaii International Conference on System Sciences.

Index ID	Source ID	Threat Vector	Threat Event	Vulnerability	Threat Agent Category	Threat Agent(s)	Potential Mitigation	Source	Reference
492	Tm1321	Failure to meet time requirements	Vbm voters may not be able to meet vbm ballot receipt deadlines due to circumstances beyond their control, thus preventing legitimate vbm ballots from being tabulated	Remote voter: faulty validation process; poorly trained election officials	human-unintentional	voter	(1) Early preparation (2) Status check process (3) Minimized the number of steps (4) Minimize duration of each step	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Pew: No Time to Vote, Challenges Facing Americas Overseas and Military Voters. January 2009, http://www.pewtrusts.org/uploadedFiles/wwwpewtrustsorg/Reports/Election_reform/NTTV_Report_Web.pdf
493	Tm1326	Correction mistake	If a vbm voter fails to follow instructions when making a correction, the ballot may be rejected.	Remote voter: faulty validation process; poorly trained election officials	human-unintentional	voter	(1) Clear rules (2) Simple procedures (3) Explicit instructions	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Yasinsac, A. and Bishop. M. (2008). The Dynamics of Counting and Recounting Votes.IEEE S&P Magazine, 6(3), 22-29. Yasinsac, A. and Bishop, M. (2008). Of Paper Trails and Voter Receipts.Proceedings of the 41st Hawaii International Conference on System Sciences.
494	Tm1327	Candidate name confusion	A vbm voter may confuse candidate names, more likely on long ballots.	Remote voter: faulty validation process; poorly trained election officials	human-unintentional	voter	(1) Voter Education	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
495	Tm1329	Mark registration system to reflect duplicate	Attacker manipulates the registration system to reflect that the voter cast another, overriding ballot.	Marked ballot: weak registration system protection	human-deliberate	malicious insider(s)	(1) Strong security protection for registration system	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
496	Tm1340	Malicious "messenger ballots"	Messenger ballots allow voters to designate another voter to pick transport votable and marked ballots in their name. attacker may [illegally] solicit applications for ballots from others and designate themselves as the authorized messenger, but vote the ballot them self.	Remote voter: weak voter authentication	human-deliberate	malicious outsider(s)	Strong voter authentication	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Sherman, Ted, "Fifth person charged with voter fraud in 2007 N.J. Senate election", The Star-Ledger, August 18, 2009, Retrieved from http://www.nj.com/news/index.ssf/2009/08/fifth_person_indicted_for_vote.html
497	Tm1341	Vote buying	Attacker pays a voter to make a particular selection. requires vote attribution.	Remote voter: susceptibility to bribery and coercion	human-deliberate	malicious outsider(s)	(1) Strong vote attribution (2) Receipt-free voting process (3) Strong legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Estep, Bill, "Clay Co. vote-buying investigation keeps expanding" Lexington Herald-Leader, Monday, May. 18, 2009 http://www.kentucky.com/181/story/799167.html
498	Tm1342	Bookie model	Attacker attracts vote sellers via word of mouth and conducts transactions individually. vbm ballots are viewed by attacker, who seals and mails envelope.	Remote voter: susceptibility to bribery and coercion	human-deliberate	malicious outsider(s)	(1) Strong vote attribution (2) Receipt-free voting process (3) Strong legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
499	Tm1343	Family member coercion attack	Voter is coerced by a family member to make selections other than their own intent.	Remote voter: susceptibility to bribery and coercion	human-deliberate	malicious outsider(s)	(1) Receipt-free voting process (2) Strong legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
500	Tm1344	Distribute false ballots	Attacker sends fake ballots to targeted voters as a denial of service.	Remote voter: limited two-way authentication	human-deliberate	malicious outsider(s)	(1) Voter education (2) Strong branding (3) Legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
501	Th3015	Damage / tamper with artifacts	Physical destruction of artifacts; tampering with artifacts	Election artifacts: access to election artifacts	human-deliberate	malicious insider(s)	physical access control , monitoring physical access	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
502	Th3016	Allocate insufficient resources	Allocate insufficient equipment or pollworkers	Voting system processes: possibility that demand for voting system resources will outstrip supply	human-unintentional	local election official	pre-election planning, contingency planning	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
503	Th3020	Educate cell captains	Educate captains in deniable ways	People being recruited: insulation of lead attacker from discovery	human-deliberate	malicious insider(s)	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
504	Th3021	Provide rewards for cell captains to distribute	Provide cell captains with rewards to distribute	People being recruited: insulation of lead attacker from discovery	human-deliberate	malicious insider(s)	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
505	Th3022	Create target list of voters to impersonate	Create target list of voters to impersonate	Voter lists: access to voter lists	human-deliberate	malicious outsider(s)	chain of custody controls on voter registration lists, if not public information	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
506	Th3028	To not make specific votes	Direct voter to not make specific votes according to attacker's demands	Eligible voter: corrupt poll worker or voter who can easily be intimidated; poll workers and poll observers unable to detect concealed ballots	human-deliberate	malicious outsider(s)	Ballot Distribution Security; Mark absentee ballots distinctly to distinguish them from ballots voted; Prevent Ballot Counterfeiting; Serial Number Ballots	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
507	Ti7999	Exploit weak password	Expose poorly chosen/protected password.	Network device, server, pc: attacker access to tools, techniques, and information	human-deliberate	malicious insider(s)	(1) Effective password selection/protection process	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007, Retrieved from http://election.dos.state.fl.us/voting-systems/pdf/SAITreport.pdf
508	Ti8000	Manipulate audit data	Create software that alters or deletes data that is intended for use in verifying the voting system's proper operation.	Voting system: access to machines / information, availability of foreign technical experts, susceptibility of vendor staff to bribery / corruption+m30	human-deliberate	malicious insider(s)	(1) High assurance software	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007, Retrieved from http://election.dos.state.fl.us/voting-systems/pdf/SAITreport.pdf
509	Ti8001	Routing attack	Manipulate the network routing infrastructure to disrupt communications in the voting system.	Pc terminal: network routing infrastructure	human-deliberate	malicious insider(s)	(1) Strong physical security	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Rubin, Avi (2002) "Security Considerations for Remote Electronic Voting over the Internet", Floram Park, NJ: AT&T Labs – Research, Retrieved from http://avirubin.com/e-voting.security.html NIST Andrew Regenscheid and Nelson Hastings, A Threat Analysis on UOCAVA Voting Systems. NISTIR 7551, December 2008, Retrieved from http://vote.nist.gov/uocava-threatanalysis-final.pdf Mote, C. D. Jr. (2002).Report of the national workshop on Internet voting: issues and research agenda. ACM International Conference Proceeding Series, 129, 1-59.
510	Ti8002	Man in the middle / pharming	Attacker masquerades concurrently as a client and server, using information from each session to accomplish objectives in the other session.	:	human-deliberate	malicious outsider(s)	(1) Strong network security	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Jefferson, D., A. D. Rubin, B. Simons, and D. Wagner. (2004). Analyzing Internet voting security.Communications of the ACM, 47(10), 59-64. Mote, C. D. Jr. (2002).Report of the national workshop on Internet voting: issues and research agenda. ACM International Conference Proceeding Series, 129, 1-59.

Index ID	Source ID	Threat Vector	Threat Event	Vulnerability	Threat Agent Category	Threat Agent(s)	Potential Mitigation	Source	Reference
511	Ti8003	Cryptanalysis	Seek to compromise the system's encryption algorithm	Network device, server, pc: attacker access to tools, techniques, and information	human-deliberate	malicious insider(s)	(1) High assurance software	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007, Retrieved from http://election.dos.state.fl.us/voting-systems/pdf/SAITreport.pdf
512	Th9904	Modify pollbooks for audit	Poll worker or election-official changes pollbooks to avoid fraud detection	Check poll book for authenticate voter, poll worker logs for precinct closeout: lack of management oversight over poll worker, election-official, auditor	human-deliberate	malicious insider(s)	audit monitoring, analysis, and reporting	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
513	Th9905	Modify logbooks and logdata used in audit	Poll worker or election- official changes logbooks and logdata to avoid fraud detection	Poll worker logs for precinct closeout : lack of management oversight over poll worker, election-official, auditor	human-deliberate	malicious insider(s)	audit monitoring, analysis, and reporting	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
514	Th9906	Because not enough spacing between candidate issues/blocks	Confuse voter into selecting wrong candidate/issue because not enough spacing between candidate / issue blocks	Validate ballot style for ballot preparation : weak reviewing process of a ballot design	human-unintentional	local election official	space different candidates / issues apart sufficiently so that voter not confused as to which response option goes with which candidate / issue	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
515	Tm9997	Attract voters with Internet adds	Attacker attracts vote sellers through blogs, message boards, Internet ads, etc.	Remote voter: susceptibility to bribery and coercion	human-deliberate	malicious outsider(s)	(1) Strong legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
516	Tm9998	Identify prospective vote sellers from voter rolls	Attacker utilizes voter rolls to identify prospective vote sellers.	Remote voter: susceptibility to bribery and coercion	human-deliberate	malicious outsider(s)	(1) Strong legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Estep, Bill, "Clay Co. vote-buying investigation keeps expanding" Lexington Herald-Leader, Monday, May. 18, 2009 http://www.kentucky.com/181/story/799167.html
517	Ti110	Manipulate accumulation data	Maliciously alter tabulation data	Machine accumulation: faulty validation process; personnel training or integrity issues	human-deliberate	malicious insider(s)	(1) High assurance software (2) Legal deterrence (3) Auditing	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Yasinsac, Alec, Breno de Medeiros, David Gainey, John Kerski, Zachary Hartley, Ryan Walega, and Michael Gerke, " Software and Security Review for Elections Systems and Software iVotronic Firmware Versions 9.1.8.0 and 9.2.0.0", Supplemental Report, For the Florida Department of State, August 14, 2007. Yasinsac, Alec, D. Wagner, M. Bishop, T. Baker, B. de Medeiros, G. Tyson, M. Shamos, and M. Burmester, "Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware, Final Report", Security and Assurance in Information Technology (SAIT) Laboratory, Florida State University, February 23, 2007. Yasinsac, Alec, John Kerski, David Gainey, Michael Gerke, Kristine Amari, and Donald Newell, "Software Review and Security Analysis of the Diebold Voting Machine Software", TSX Supplement, For the Florida Department of State, September 28, 2007.
518	Th10000	By omitting use of bold	Omit bold text to help voters differentiate between voting tasks	Validate ballot style: weak reviewing process of a ballot design	human-deliberate	malicious insider(s)	bold certain text, such as office name to help voters to differentiate between voting tasks	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Norden, Lawrence, Kimball, David, Quesenbery, Whitney, and Chen, Margaret (2008) "Better Ballots." July 20 2008, Retrieved from Brennan Center for Justice, http://www.brennancenter.org/content/resource/better_ballots
519	Th10001	Purchase or coerce vote	Motivate voters to either (a) stay away from polls or (b) vote in compliance with attacker demands	Eligible voter, signed in voter: susceptibility of voters to buying and coercion; breach of voter privacy; ability to attribute vote	human-deliberate	malicious outsider(s)	maintain voter privacy; limit access to polling place	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Dekel, Eddie, Matthew O. Jackson, Asher Wolinsky (2004) Vote Buying, Revision: October 19, 2004, Retrieved from http://else.econ.ucl.ac.uk/newweb/esrc_seminars/nov2004/dekel.pdf Fund, John (2004) "Democracy Imperiled: America's election problems," National Review Online, September 13, 2004, Retrieved from http://www.nationalreview.com/comment/fund200409130633.asp. Jones, Doug W. (2005) University of Iowa, Threats to Voting Systems, NIST workshop on Threats to Voting Systems, 7 October 2005, Gaithersburg, MD, Retrieved from http://vote.nist.gov/threats/papers/threats_to_voting_systems.pdf
520	Ti112	Manipulate randomization	Attacker compromises randomization algorithm to alter votes or tabulation.	Audit results: lack of transparency, oversight; inability to detect or recover	human-deliberate	malicious insider(s)	(1) High assurance software (2) Legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007, Retrieved from http://election.dos.state.fl.us/voting-systems/pdf/SAITreport.pdf
521	Th10002	Promise to punish	Promise some form of punishment in order to coerce voter	Eligible voter, signed in voter: susceptibility of voters to intimidation; lack of voter privacy	human-deliberate	malicious outsider(s)	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and poll workers	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Van Acker, Bernard (2004), Remote e-Voting and Coercion: a Risk-Assessment Model and Solutions, 2004, Retreived from http://subs.emis.de/LNI/Proceedings/Proceedings47/Proceeding.GI.47-6.pdf
522	Th10003	Use cell captains to execute deniable impersonation threat	Use cell captains to execute deniable impersonation attack	Authenticate voter, ,: political influence / power of political leaders or election officials	human-deliberate	malicious insider(s)	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
523	Th10005	Perform voter impersonation threat	Perform voter impersonation threat	Voting system, ,: accessibility of lists of voters not likely to vote; soft voter authentication process; poll workers don't know voters; willingness of poll workers to engage in fraud	human-deliberate	malicious outsider(s)	media protection policy and procedures, personnel security, access control, audit and accountability, identification and authentication	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	LTM-USA Delivery-01 (2009) LTM Election Threat Models, Lazarus Technology Mentoring, Inc.
524	Th49	Subvert no-show vote	Ballot manipulation prior to tabulation - ballot box stuffing - stuffing after the polls close	Check poll book for authenticate voter: unsecured poll book; corrupt official who coerces other poll workers	human-deliberate	malicious insider(s)	limited/no access to the ballot boxes to the poll workers after the polls close improve administration of the poll workers on the election day	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
525	Th10007	Subvert audit	Render routine statistical audit ineffective	Election artifacts: no separation of duties; control by election officials over audit procedures, access to election artifacts	human-deliberate	malicious insider(s)	data protection policy and procedures, physical and environmental protection, personnel security, system and information integrity, access control, audit and accountability, identification and authentication	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	LTM-USA Delivery-01 (2009) LTM Election Threat Models, Lazarus Technology Mentoring, Inc.
526	Th10008	Discourage voters	Intentionally discourage voters from voting	Checking, check poll book, authenticate voter: unwillingness or inability of voters to appeal poll workers' decisions	human-deliberate	malicious outsider(s)	personnel security, multi-person, multi-party controls, transparency of process, election law governing polling place operations, voter awareness and training, auditing and accountability, physical and environmental controls at the polling place	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
527	Ti55	Alter ballot creation software	Attacker alters the system used to generate ballot formats, either causing malformed ballots or to allow external control for ballot faults.	Network server: poor security during election artifacts delivery, insecure voter technology	human-deliberate	malicious insider(s)	(1) Strong physical security of devices (2) Poll worker background checks (3) Strong legal deterrence (4) High assurance software	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007, Retrieved from http://election.dos.state.fl.us/voting-systems/pdf/SAITreport.pdf

Index ID	Source ID	Threat Vector	Threat Event	Vulnerability	Threat Agent Category	Threat Agent(s)	Potential Mitigation	Source	Reference
528	Ti57	Phishing attack	Attracting a voter to a malicious voting web site.	Remote voter: susceptibility to bribery, coercion, and deception	human-deliberate	malicious outsider(s)	(1) Voter training (2) Strong legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Rubin, Avi (2002) "Security Considerations for Remote Electronic Voting over the Internet", Floram Park, NJ: AT&T Labs – Research, Retrieved from http://avirubin.com/e-voting.security.html NIST Andrew Regenscheid and Nelson Hastings, A Threat Analysis on UOCAVA Voting Systems. NISTIR 7551, December 2008, Retrieved from http://vote.nist.gov/uocava-threatanalysis-final.pdf
529	Th10014	Select audit units before election	Audit manipulation - select audited items dishonestly	Validate precinct results: lack of basic audit in effect	human-deliberate	malicious insider(s)	implement a more transparent and publicly observable random selection process, with clear written procedures or guidelines	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Mail)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
530	Ti58	Attract the voter	Tricks voters to visit the malicious web site.	Remote voter: susceptibility to bribery, coercion, and deception	human-deliberate	malicious outsider(s)	(1) Voter training (2) Strong legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Rubin, Avi (2002) "Security Considerations for Remote Electronic Voting over the Internet", Floram Park, NJ: AT&T Labs – Research, Retrieved from http://avirubin.com/e-voting.security.html
531	Th10015	Publish bogus audit results	Penetrate jurisdiction web site and publish bogus audit results to hide attack	Canvass, official report, report results: lack of publishing system security that leads to obscure results	human-deliberate	malicious insider(s)	increase security in both areas - tabulator and publication website	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
532	Ti59	Alter the voting session	Malware alters the voter's interaction to accomplish their malicious act.	Remote voter: susceptibility to bribery, coercion, and deception	human-deliberate	malicious insider(s)	(1) High assurance software (2) Auditing	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Rubin, Avi (2002) "Security Considerations for Remote Electronic Voting over the Internet", Floram Park, NJ: AT&T Labs – Research, Retrieved from http://avirubin.com/e-voting.security.html
533	Th10016	Add new fraudulent evidence	Replace real votableballots with votableballots designed to match the hand counted and audit in warehouse; results manipulation	Votable ballots: access to votable ballots	human-deliberate	malicious insider(s)	add more security features to the real VotableBallots to discourage attackers to duplicate VotableBallots, implement chain of custody and strong physical security	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
534	Ti61	Alter the ballot	Malware reports other than the voter's selections for tabulation.	Remote voter: susceptibility to bribery, coercion, and deception	human-deliberate	malicious insider(s)	(1) High assurance software (2) Auditing	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
535	Th10017	Misguide auditors	Give improper instructions to auditors to render audit ineffective	Validate precinct results: poor policies allows election official to specify their own rules	human-deliberate	malicious insider(s)	revise policies to ensure that ElectionOfficial follows the guidelines for auditing process	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
536	Ti62	Collect voter information	Malware collects voter information for later malicious election related use.	Not modeled: susceptibility to bribery, coercion, and deception	human-deliberate	malicious insider(s)	(1) High assurance software	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
537	Th10018	Audit insufficient sample	Audit manipulation - audit insufficient of sample to avoid tampered audit unit detected	Validate precinct results: poor auditing practices or procedures	human-deliberate	malicious insider(s)	revise auditing practices or procedures to audit manipulation	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
538	Ti63	Voter impersonation attack	Attacker assumes the identity of a legitimate voter.	Remote voter: personnel training or integrity issues; faulty authentication	human-deliberate	malicious outsider(s)	(1) Strong voter authentication (2) Strong legal deterrence	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Jefferson, D., A. D. Rubin, B. Simons, and D. Wagner. (2004). Analyzing Internet voting security.Communications of the ACM, 47(10), 59-64.
539	Th10019	Exploit variation in batch sizes	Audit manipulation - random sampling from large variation of audit unit size minimize the risk of detection	Validate precinct results: poor auditing practices or procedures	human-deliberate	malicious insider(s)	revise auditing practices or procedures to audit manipulation	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
540	Ti64	Steal voters' password	Attacker steals a legitimate voter's password.	Remote voter: weak passwords and susceptibility to bribery, coercion, and deception	human-deliberate	malicious outsider(s)	None provided in reference.	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
541	Th10020	Establish single contest audit rule	Election law manipulation - select a race randomly - assume audit untampered race only	Validate precinct results: poor election laws / policies / guidelines	human-deliberate	malicious insider(s)	revise election law or regulation to audit more than one race	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD. LTM-USA Delivery-01 (2009) LTM Election Threat Models, Lazarus Technology Mentoring, Inc.
542	Ti65	Vote for relative	Malicious party masquerades as a family member or coercively submits a relative's ballot.	Remote voter: personnel training or integrity issues; faulty authentication	human-deliberate	malicious outsider(s)	None provided in reference.	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
543	Th10021	Arrange contest audit	Arrange selection of a non-subverted contest for audit	Validate precinct results: poor election laws / policies / guidelines	human-deliberate	malicious insider(s)	revise election law or regulation to audit more than one race	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
544	Th10022	Select audited items before commit	Tabulation manipulation - clean up data automatically based on poll worker	Election artifacts: lack of tabulation server security	human-deliberate	malicious insider(s)	increase security features of tabulators	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
545	Th10023	Tamper with audit totals	election results manipulation - precinct total do not add up to poll totals	Precinct accumulation, precinct audit data: poor auditing practices or procedures	human-deliberate	malicious insider(s)	implement a more transparent and publicly observable random selection process, with clear written procedures or guidelines	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD. Norden, Lawrence D.(Chair) (2006) "The Machinery of Democracy: Protecting Elections in an Electronic World", Brennan Center Task Force on Voting System Security, Voting Rights & Election Series, 2006, Brennan Center for Justice at NYU School of Law, Retrieved from http://noleakybuckets.org/brennan/securityfull7-3reduced.pdf
546	Th10024	Avoid correction	When audits reveal mismatches, avoid calling for a recount or other corrective measures by making excuses; election results manipulation - give reasons for mismatch - avoid recount, and fraud audit items detection	Validate jurisdiction results: poor election laws / policies / guidelines	human-deliberate	malicious insider(s)	implement a policy that requires ElectionOfficial to give non-obscure reasons for result discrepancies and take corrective measures to avoid fraud	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
547	Ti70	Other systematic selection	Attacker identifies prospective targets that maximize their masquerade success.	Remote voter: personnel training or integrity issues; faulty authentication	human-deliberate	malicious insider(s)	None provided in reference.	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	EAC. (2010). Election Operations Assessment - Threat Trees and Matrices and Threat Instance Risk Analyzer (TIRA) Draft Report.
548	Th10026	Overwhelm audit observers	Overwhelm observers with too many auditors - auditor manipulation - incompetent auditors ballot manipulation - dishonest audit	Validate precinct results: lack of management oversight over election officials and auditors	human-deliberate	malicious insider(s)	implement a policy that specifies only certain number of Auditors can be employed so that Observers can perform their duty efficiently	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.

Index ID	Source ID	Threat Vector	Threat Event	Vulnerability	Threat Agent Category	Threat Agent(s)	Potential Mitigation	Source	Reference
549	Th10027	Destroy electionartifacts	Physically destroy electionartifacts, including ballot destruction	Deliver to jurisdiction: poor security during election artifacts delivery	human-deliberate	malicious insider(s)	Implement chain of custody and strong physical security during delivery	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD. Norden, Lawrence D.(Chair) (2006) "The Machinery of Democracy: Protecting Elections in an Electronic World", Brennan Center Task Force on Voting System Security, Voting Rights & Election Series, 2006, Brennan Center for Justice at NYU School of Law, Retrieved from http://noleakybuckets.org/brennan/securityfull7-3reduced.pdf
550	Ti76	Verify the vote	Vote buyer confirms that the vote seller accomplished the agreed action.	Remote voter: susceptibility to bribery and coercion	human-deliberate	malicious outsider(s)	(1) Receipt-free voting system	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Jefferson, D., A. D. Rubin, B. Simons, and D. Wagner. (2004). Analyzing Internet voting security.Communications of the ACM, 47(10), 59-64.
551	Th10028	Vote in place of voter	Impersonate and vote in the place of an eligiblevoter; a list of voters who are unlikely to vote may be prepared and people may be recruited to vote for that person. a polling place where a poll workers are not likely to know voters may be targeted.	Authenticate voter: access to lists of voters not likely to vote; poll workers don't know voters; corrupt poll worker	human-deliberate	malicious outsider(s)	require Credentials at polling places; conduct precise and careful purges on voter lists to remove duplicate names, people who have moved, died, or are otherwise ineligible.	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
552	Ti77	Make the payment	Vote buyer transfers payment to the vote seller.	Remote voter: susceptibility to bribery and coercion	human-deliberate	malicious outsider(s)	None provided in reference.	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Estep, Bill, "Clay Co. vote-buying investigation keeps expanding" Lexington Herald-Leader, Monday, May. 18, 2009 http://www.kentucky.com/181/story/799167.html
553	Ti84	Insider attacks	Malicious actions that may be taken by elections insiders, such as officials or poll workers.	Voting system: susceptibility to bribery and coercion	human-deliberate	malicious insider(s)	(1) Election official background checks (2) PW background checks (3) Strong legal deterrence (4) Two person integrity	Election Assistance Commission - Draft Election Operations Assessment Report (Vote by Internet)	Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, " Software Review and Security Analysis of the Diebold Voting Machine Software," Final Report For the Florida Department of State, July 27, 2007, Retrieved from http://election.dos.state.fl.us/voting-systems/pdf/SAITreport.pdf
554	Th10030	Motivate voter	Use payment, persuasion, or coercion to enlist the cooperation of subvertible voters	Voter: human susceptibility to being bribed or coerced	human-deliberate	malicious outsider(s)	personnel security, including strong laws against vote fraud, sanctions against violators and colluders, background checks, awareness and training for voters and poll workers, physical and environmental protection, limiting access to polling place and providing polling place patrols	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, D. W. (2005, October).Threats to voting systems. Position paper for the NIST workshop on Threats to Voting Systems, Gaithersburg, MD.
555	Th10031	Recruit attackers among legalvoters	Subvertible voters are gathered to increase the impact of chain voting or a group of attackers carry out chain voting attack	Legal voters: susceptibility of voters to being bribed or intimidated	human-deliberate	malicious outsider(s)	personnel security, including strong sanctions/laws against violators, and background checks, multi-person, multi-party controls, awareness and training for potential insider recruits	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, Doug W. (2005) Chain Voting, August 26, 2005.
556	Th10032	Acquire votableballot	An outside attacker smuggles a votableballot or an election insider takes an absentee ballot and uses it for chain voting	Ballot stock: lack of polling place security	human-deliberate	malicious insider(s)	chain of ballot custody procedures, polling place security, including observers	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, Doug W. (2005) Chain Voting, August 26, 2005.
557	Th10033	Vote with pre-marked ballot	Subverted voter takes markedballot to polling place and votes with it, while also legally obtaining votableballot	Commit ballot: lack of polling place security; voter privacy measures helps attacker conceal ballots	human-deliberate	malicious insider(s)	chain of ballot custody procedures, polling place security, including observers	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, Doug W. (2005) Chain Voting, August 26, 2005.
558	Th10034	Remove votableballot out	Voter removes votableballot out of polling place and takes it to attacker to enable next cycle of chain voting	Ballot stock: lack of polling place security; voter privacy measures helps attacker conceal ballots	human-deliberate	malicious insider(s)	chain of ballot custody procedures, polling place security, including observers	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Jones, Doug W. (2005) Chain Voting, August 26, 2005.
559	Th10035	Pay for candidate support	Make a direct payment to voters to support a particular candidate; attacker promises to bribe voters if they prove the attacker with evidence that they voted to the particular candidate supported by attacker.	Eligible voter, signed in voter: susceptibility of voters to bribery	human-deliberate	malicious outsider(s)	Educate the voters about the importance of voting	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Fund, John (2004) "Democracy Imperiled: America's election problems," National Review Online, September 13, 2004, Retrieved from http://www.nationalreview.com/comment/fund200409130633.asp. Dekel, Eddie, Matthew O. Jackson, Asher Wolinsky (2004) Vote Buying, Revision: October 19, 2004, Retrieved from http://else.econ.ucl.ac.uk/newweb/esrc_seminars/nov2004/dekel.pdf
560	Th10036	Intimidate to suppress turnout	Coerce the voter to stay away from polls with threats and intimidation	Eligible voter: susceptibility of voters to intimidation; lack of voter privacy	human-deliberate	malicious outsider(s)	awareness and training, strengthen the election law against such crimes	Election Assistance Commission - Draft Election Operations Assessment Report (Hand-Counted Paper Ballot)	Van Acker, Bernard (2004), Remote e-Voting and Coercion: a Risk-Assessment Model and Solutions, 2004, Retrieved from http://subs.emis.de/LNI/Proceedings/Proceedings47/Proceeding.GI.47-6.pdf
561	A0001	Penetration attack	A malicious individual uses a trojan horse or remote control program to transport a malicious payload to its target host computer client or server.	Encryption and authentication mechanisms, e.g. encryption and authentication not designed to detect penetration.	human-deliberate	malicious outsider(s)	Suitable intrusion detection programs.	Internet Policy Institute	Jefferson, D., Rubin A. for IPI. (2001) Report of the National Workshop on Internet Voting: Issues and Research Agenda
562	A0002	Denial of service and ddos attacks	Interruption of the communication between a client and a server by flooding the target with a number of requests exceeding its bandwidth.	Weak authentication between client and server.	human-deliberate	malicious outsider(s)	Strong authentication protocol; greater bandwidth and redundant servers	Internet Policy Institute	Jefferson, D., Rubin A. for IPI. (2001) Report of the National Workshop on Internet Voting: Issues and Research Agenda
563	A0003	Spoofing attack	A malicious insider creates a spoofed voting website, masquerading as a legitimate one to spy on or steal a voter's vote, or prevent a voter from casting his/her ballot.	Outdated security protection on client and server systems; poor training or education in distinguishing between a spoofed website and the legitimate one.	human-deliberate	malicious outsider(s)	Up-to-date security measures on client and server systems and education of voters.	Internet Policy Institute	Jefferson, D., Rubin A. for IPI. (2001) Report of the National Workshop on Internet Voting: Issues and Research Agenda
564	A0004	Incompatible hardware/software on the client side	A voter is unable to conduct transactions with the voting software due to incompatibility of his/her software or hardware.	Some voters may have hardware and/or software incompatible with the voting application/web ivoting interface.	human-unintentional	voter	Ensure that the voting application can be run on a diverse group of system configurations.	Congressional Research Service	Coleman, K. (2002) CRS. Report to Congress: Internet Voting
565	A0005	Lack of access to computer hardware with Internet connectivity	The voter does not have access to a computer with Internet connectivity.	The voter does not own nor have ready access to a computer with Internet connectivity	human-unintentional	voter	Ensure that all registered UOCAVA voters have access to computer hardware with Internet connectivity.	Congressional Research Service	Coleman, K. (2002) CRS. Report to Congress: Internet Voting
566	A0006	Exploit of lack of technical know-how at the leo	A malicious insider manipulates election artifacts (forms and instructions).	Lack of technical expertise at the leo	human-deliberate	malicious insider(s)	More uniform training and countermeasures to ensure that tampering be detected.	Election Assistance Commission	EAC. (2007). UOCAVA Voters and the Electronic Transmission of Voting Materials in Four States - Draft
567	A0007	Local election officials make errors while operating the remote absentee electronic voting system.	Staff at the leo make mistakes affecting forms and instructions while operating the remote absentee electronic voting system.	Lack of technical expertise at the leo	human-unintentional	local election official	More uniform training and outreach in understanding and operating the remote absentee electronic voting system.	Election Assistance Commission	EAC. (2007). UOCAVA Voters and the Electronic Transmission of Voting Materials in Four States - Draft
568	A0008	Loss of data during network connectivity interruption	A voter loses the information entered during his/her voting session due to network connectivity interruption	Requirement for continuous network connectivity during voting session.	human-unintentional	mail employee; ISP technician	Redundancy built in the voting system to prevent connectivity interruption to the voting server.	Florida Department of State	Hall et al. (2008). Software Review and Security Analysis of Scytl Remote Voting Software
569	A0009	Malware injection into the mixing service compromising ballot anonymity.	A malicious individual with authorized access to the mixing service might be able to introduce malware onto the mixing service. machine	Integrity of local election officials; lack of security and supervision at the leo.	human-deliberate	malicious outsider(s)	Malware and intrusion detection system on mixing service equipment.	Florida Department of State	Hall et al. (2008). Software Review and Security Analysis of Scytl Remote Voting Software
570	A0010	Non-random number generation in ballot identifiers on voting clients	A malicious insider injects a malware on the voting client instructing it to choose ballot identifiers non-randomly to allow for compromise of voter's anonymity.	Susceptibility of the voting client to malware injection.	human-deliberate	malicious outsider(s)	Malware and intrusion detection system on voting client.	Florida Department of State	Hall et al. (2008). Software Review and Security Analysis of Scytl Remote Voting Software
571	A0011	Electronic voter receipt does not allow for a voter to verify that his/her vote was counted as cast.	A voter is provided access to the list of ballot identifiers linked to counted votes but cannot verify that his/her choice was counted as intended.	Lack of voter verifiability on electronic voter receipts	human-unintentional	local election official	Allow the voter to securely check the choice counted in reference to his/her ballot identifier, after the election has ended, to prevent vote buying.	Florida Department of State	Hall et al. (2008). Software Review and Security Analysis of Scytl Remote Voting Software

Index ID	Source ID	Threat Vector	Threat Event	Vulnerability	Threat Agent Category	Threat Agent(s)	Potential Mitigation	Source	Reference
572	A0012	Exploit weak cryptography for malicious aims.	A malicious insider exploits weak cryptography to tamper with election materials.	Weak cryptography in the remote absentee electronic voting system.	human-deliberate	malicious outsider(s)	Military-grade cryptography; Separation of keys.	Florida Department of State	Hall et al. (2008). Software Review and Security Analysis of Scytl Remote Voting Software
573	A0013	Exploit of Internet vulnerability to intercept voting communications	A malicious outsider with Internet access exploits existing Internet vulnerabilities to gain access to voting information during their transmission between the voter and the leo.	Existing Internet vulnerabilities relevant to the voting syste,.	human-deliberate	malicious outsider(s)	Military-grade cryptography; Military-grade secure network;	Florida Department of State	Hall et al. (2008). Software Review and Security Analysis of Scytl Remote Voting Software