VVSG Ad Hoc Committee Report – February 2, 2010:

QUESTION: Are there any glaring risks or mitigations missing from the Risk Trees?

- 2-8 DRE (Page 21) - May want to add a node addressing the compromising of flash cards and Personal Electronic Ballots (ES&S system).

- 2-10 DRE Ballot Design (Page 23) - Not enough spacing between candidate/issue blocks, voters may inadvertently select wrong response.

- In jurisdictions that provide a short window of time in which to accept or reject provisional ballots, ballots could be "selectively" reviewed by election officials thereby leaving certain ballots unreviewed and subsequently rejected due to not being reviewed in the time period provided by state law.

- Pg. 19, Section 2.2.2.9 - errors in ballot adjudication.

- In jurisdictions that provide a short window of time in which to accept or reject provisional ballots, ballots could be "selectively" reviewed by election officials thereby leaving certain ballots unreviewed and subsequently rejected due to not being reviewed in the time period provided by state law.

- For DRE: Many states now require a voter-verifiable paper audit trail (VVPAT) and in some states, the VVPAT is considered the official ballot. I did not see any threat or risk associated with an attack on the VVPAT.

- For DRE: Under disrupt operations, disruptions from environmental events, there should be a threat of power failure.

- For PCOS: I did not see any threat or risk associated with an attack on the transmission of election results. The PCOS can tabulate the results at the precinct level and transmit the precinct results, via telephone modem, to the host tabulator.

- The decision to base the DRE threat tree on the assumption that only an electronic ballot image exists (i.e. no VVPAT) should be reconsidered as a substantial number of states either require a VVPAT or encourage its use. If threats to the VVPAT are included, printer malfunction such as paper jams, illegibility of the paper record or inaccurate reflection of the voter's choices should be considered.

QUESTION: How useful were the instructions provided?

- If "instructions" means § 1 of report, I think that the section was written assuming that the reader had an understanding of threat trees and matrices, etc. I think a "plain English" explanation would be helpful.

- The instructions provided some context, but were not sufficient without the demonstration.

QUESTION: Was the tree structure consistent throughout all voting technologies?

- There are inconsistencies in the tree structure between DRE , PCOS and CCOS. The tree structure for PCOS included the category "commit errors in operations" with several subcategories. The tree structure for DRE did not include this category, however, it did include several of the subcategories listed under "commit errors in operations" on the PCOS tree under the "perform insider attack" category such as "attack other than polls - confuse voters with poor ballot design" and the "perform insider attack - discourage voters -create long lines". Many of the items on the PCOS tree structure under "commit errors in operations" would apply to both the PCOS and DRE technologies and should be consistent on the tree structures. Another example is under "subvert voting process" on the PCOS tree structure, buy or coerce vote, pay candidate for support, use drugs, alcohol as payment. The DRE structure doesn't break down the buy or coerce vote subcategory in the same way. In addition, the CCOS tree structure included categories not on the PCOS tree structure and terminology used in the structure was slightly different than the PCOS tree structure. PCOS and CCOS are very similar and should have similar nodes on the tree structures.

QUESTION: Were any of the risks identified non-applicable or out of scope?

- Discouraging voters seems far afield from assessing the voting equipment.

- Commit Vote Fraud attack should be limited to attack through voting equipment/process, not vote buying and impersonation attacks.

- Attacking audit should also be limited to attack through the voting equipment/process, not compromising auditors, publishing bogus audit results, etc.

- For example, vote buying is unrelated to the voting system and would seem to be out of scope. Similarly, some of the issues with the check-in process (i.e., selectively challenging voters, falsely rejecting the ID check, work slowly) and "subvert voting process (i.e., exploit Electoral College rules) seem unrelated to the voting system.

- EAC staff indicated on a teleconference with the VVSG Ad-Hoc group that the purpose of this threat assessment and risk analyzer was for EAC to use it as a tool when developing the VVSG for testing and certification of voting equipment. With this in mind, there appears to be numerous threats that are more associated with the overall electoral process than specifically with voting system technology. If this is being used as a tool for developing voting system standards, it should be limited to those threats and risks directly associated with use of and operations of the equipment, not threats to the overall electoral processes such as rejecting voter registration or fraudulent registrations, sending voter to wrong polling place, or using drugs or alcohol to buy or coerce votes. Threats directly related to overall electoral processes, such as voter registration and the conduct of candidates, may impact the outcome of an election but they are distinctively different types of threats than threats associated with the use of voting technologies.

- Terms such as "voter confidence" (which is in the glossary twice), "voter intimidation/coercion", "vote buying" are inappropriate in a document for which the primary purpose is to assist the EAC, NIST and the TGDC in development of guidelines for electronic voting systems.

- Similarly, if this document is primarily to assist the EAC, NIST and the TGDC in development of the VVSG the threat trees for hand-counted paper ballots and vote by mail would appear to be outside the scope.

- The recommended controls in the threat matrices appear to be primarily administrative in nature and therefore outside the scope of project if it is limited to assisting the EAC, NIST and the TGDC in developing the VVSG.

QUESTION: Did the explanations of the risk activities contain correct terminology and objective language?

- Section 2 - DRE Pg. 20 - Paragraph 1 of the introduction states that the model assumes that the DRE is precinct based and does not use a VVPAT, but Node 2.2.1.1.3.2 contains language contrary to that statement. The Node (discourage voters) is described as "program the VVPAT to exhaust the paper supply". The matrix then expands the definition to state that malware could be installed that would cause the paper supply to be exhausted and would delay the opening of the polls. DRE voting equipment without VVPAT use a printer with a paper roll, but it is not a VVPAT. The printer simply prints an opening and closing tape of accumulated vote totals for the voting unit.

- Section 4 - Central Count Optical Scan Pg. 153 - Paragraph 2 states that using CCOS voters do not have the capability to have over and under votes detected. Because optical scanners can be programmed to detect over and under votes at any time, a more accurate statement would be that voters do not have the ability to have over and under votes detected in their presence.

- Within the tree structures, there are variations in terminology. For instance, on the CCOS tree, 3.2.1.1.3 is create long lines, with 3.2.1.3.1 stymie voters by intentionally working slowly. This same threat is on the DRE and PCOS tree but worded differently. If there is going to be a threat for creating long lines, the terminology and threats used should be consistent throughout these technologies.

- As noted in the question on scope, some terms in the glossary and in the threat trees are not objective.

- It is not clear whether absentee/remote voting include early voting and voting before Election Day at a vote center or the local election authority's office

QUESTION: Was the same level of detail of risk applied to each voting technology?

- There are inconsistencies with the tree structure between DRE, PCOS and CCOS and with the inconsistency, there are different levels of risks applied to each tree structure. For instance, on the DRE tree under subvert voting process, commit vote fraud attack, there are more levels of detail for this risk than listed under PCOS or CCOS for the same type of risk, commit vote fraud attack.   There needs to be a thorough review of these three tree structures to ensure consistent structures, terminology and level of detail is applied.

- The threat tree on internet voting appears to contain significantly less detail that the threat trees for PCOS, CCOS and DREs

- If this document is intended to assist the EAC, NIST and the TGDC in development of the VVSG, are internet voting and vote by phone included because standards for them will be included in the VVSG?

QUESTION: Were there terms that you didn't understand that need to be defined?

- Glossary definition of Partisan Office is not quite right. The nature of a partisan office allows candidates to run by party, but independent candidates (or those not belonging to any party) can still be a candidate for a partisan office.

- Vote Flipping is listed twice on page 328.

- Voter Purging definition. There is allowable purging of the voter rolls. If this is meant to be a type of voter suppression, then the definition should include that a voter was intentionally purged from the voter roll when not allowable by law.

- It might be helpful to readers to define terms used in the descriptions of the process such as "acyclic". The terms in the definition of "perturbation analysis" should be defined.

QUESTION: Which of the three formats of presentation of the trees did you find easiest to follow? Is there another format that you think should be used?

- Threat tree is easiest. Then outline, then matrix.

- I though the threat tree - graphics were the easiest to understand. It would be helpful to include a reference to § 11 (Key to Graphical Threat Tree Symbols) on each threat tree graphic so the reader know immediately where to go to find out what the symbols represent.

- I found both tree structures to be easy to follow.

- I found the graphic representation to be the easiest to follow, although the additional information such as the threat description in the threat matrix was sometimes helpful.

QUESTION: Did you have any other comments?

- The vocabulary seems complicated. While it is understood that the document will be used by system analyst, the documents should be easier to read for the layman.

- Some language seems inflammatory - such as the term "vote stealing" - consider substituting less inflammatory language such as "compromise the integrity of the ballot" instead. Also the word attack is used constantly - also inflammatory.

- The nature of the document is that risks are constantly evolving. What will be the maintenance process for the document?

- In §§ 1 (Introduction section) and 11, the symbols are referred to as "nodes," but in §1.3, the phrase "gate" is used. Are "nodes" and "gates" the same? If so, please use the same term. If not, please describe what "gates" are § 11.

- Continue to emphasize that the election operations assessment is a tool for the U.S. Election Assistance Commission, NIST, the TGDC, etc. to develop future Voluntary Voting System Standards.

- On the whole, we thought these were very useful. We reviewed only the DRE threat tree, but it seemed very complete and we really liked the recommended controls. This could be useful to states and local jurisdictions in setting up proper controls and check lists.

- To actually validate that every risk and every control that was identified would be very time consuming. Is that what you are wanting the VVSG to do? If so, we probably need to broaden the membership of this committee to ensure that all 7 voting system operations are adequately covered. In addition, we probably need face to face meetings.

- The EAC may want to make sure that the EAC Management Guidelines address all the recommended controls.

- To be truly useful to county and local election officials, a “gateway” or some other simpler kind of document would be needed to help a local jurisdiction use the information.

- Not sure that this will be useful as a tool for local jurisdictions. Two counties in Texas with the same voting system could theoretically come up with vastly different results. Seems like this is a tool the EAC should use and set a national benchmark.

- Probably would have to release to the public because TIRA does not appear to expose any security issues, but again, the EAC (with input from relevant stakeholders) should probably be the entity to set the values. Others could use the tool and come up with different results, but at least EAC would have set the federal expectation. Or, perhaps EAC could adopt the values as determined by the University of South Alabama and their partners?

- I am concerned that because TIRA "allows the evaluator to quantify the stakeholder's intuition" and uses variable based on the stakeholder's "perception" that the product is too dependent on the subjective views of the analyst/evaluator or the stakeholder.

- The project requires documentation so that the EAC and the election community can use and maintain the risk assessment tools without the assistance of specialized experts. However the demonstration I witnessed broke down because something had been changed in the tool after a previous successful demonstration.

Typographical or Grammatical Errors

TREE

- Pg 1, Paragraph 1, Line 3 - change "effor1" to effort
- Pg 5, Paragraph 2 - change the word "tress" to trees
- Pg. 6 bottom of page - insert a line between the last two paragraphs
- In Sections 1.4 and 1.5 of the Introduction to Threat Trees and Matrices there inconsistencies using the wording "800 dash 30" and "800-30".

MATRIX

TIRA

OTHER

- INTRODUCTION - Page 1, first paragraph, second sentence "effort **1** to catalog"
- § 1, page 1: In the third line, "effort1" should be effort. If the "1" is supposed to be a footnote, where are the footnotes?
- § 1, page 2: should the 3rd bullet be "Detectability" rather than "Delectability"?
- § 1.3, page 5: The first line includes the following: "t e've also got nonhuman." Correct as appropriate. In the first line under "Usefulness of Sub-tree Classification," "tress" should be "trees."
- § 1.4, page 5: The beginning of Threat Trees - Outline refers to the "second way" but this is the first one listed. Should it be the "first way"?
- PROJECT GLOSSARY - "Contest Vote Totalss" is a typo within definition of Spoiled Ballot