WRITTEN TESTIMONY OF ALEC YASINSAC, PH.D.

SCHOOL OF COMPUTER AND INFORMATION SCIENCES

UNIVERSITY OF SOUTH ALABAMA

BEFORE THE

U. S. ELECTION ASSISTANCE COMMISSION

PUBLIC MEETING: IDENTIFYING AND MITIGATING RISK IN ELECTIONS

My name is Alec Yasinsac. I am Professor and Dean of the School of Computer and Information Sciences at the University of South Alabama. I previously served on the faculty at Florida State University for nine years, after serving twenty years in the United States Marine Corps. I am co-founder of the Security and Assurance in Information Technology (SAIT) Laboratory where I led several voting system security reviews for the State of Florida.

Thank you for the opportunity to address this public meeting of the EAC. I am here today representing the investigators for the EAC's election operations assessment project and my comments relate to that project. Our final report and the other deliverables are the authoritative project data. My comments here are intended to summarize and highlight, rather than supplement, data in those deliverables.

In September 2008, the Election Assistance Commission (EAC) conducted a procurement to obtain the services of an inter-disciplinary team to perform a scientifically founded Voting System Risk Assessment. The University of Southern Alabama team was competitively selected to conduct the requested analysis.

The notion of "risk" is straightforward: it is a collective computation of the likelihood and prospective impact of a fault or failure. The challenge for this project was to provide the EAC actionable risk data; that is, to provide resources that will allow the EAC to rigorously analyze voting system risks and to then use that analysis to make corresponding, well-founded decisions relative to voting system standards. The Project Team's efforts were driven exclusively by that goal.

Three tasks were necessary to achieve the desired outcome:

1. Establish a reference model as a foundation for analysis
2. Identify generic voting system threats and
3. Develop a risk assessment approach that is appropriate for the required analysis.

The Project Team first created a set of reference models that included detailed descriptions of the voting terms, processes, actors, etc. The investigatory team delivered those descriptions and models in early 2009, and after extensive review, they were accepted by the EAC in May 2009.

The second task was to identify generic threats associated with each of seven selected voting technologies. The investigatory team captured the outcome of this work as a set of threat trees using NIST 800-30 threat definitions, creating one threat tree for each selected technology type. These threat trees are documented within our final report and give the EAC a solid foundation for beginning a formal risk assessment process.

The project's ultimate goal was to develop a tool to assist the EAC in evaluating voting system risks and to facilitate cost-benefit analysis on the potential mitigations for identified threats. The investigators developed the Threat Instance Risk Analyzer (TIRA), for that purpose. TIRA is described in detail in the report, but it is important to note that TIRA has two fundamental properties.

1. First, TIRA is designed to capture the expertise of the analyst in a way that the analyst's decisions can be reviewed, debated, and adjusted. During the review process, we found that TIRA facilitates team analysis that can synergistically capture the cumulative voting system expertise of an analysis team.

2. TIRA's second fundamental property is that its analysis is exclusively comparative. That is, TIRA's result is a unit-less number that is meaningless by itself. Value is only gained through comparative analysis that allows the analyst to assess, for example, the relative merits of incorporating two different controls to mitigate a threat in a voting system.

My comments so far have described what the project deliverables *are* designed to do. The following comments relate to things that our deliverables are *not* intended to be.

1. This project is not intended to be a comprehensive threat analysis. While the team conducted extensive research to identify voting system threats for this project, there is essentially an infinite number of possible threats for any non-trivial voting technology. The threats that we present were found in the literature or news articles or were derived through the expertise of the Project Team and the many reviewers that have commented on the threat trees. Nonetheless, we do not claim that we have captured all relevant threats.

2. This project did not analyze risk for any specific, operational voting system. The threat trees were designed at a high abstraction level and represent a starting point for voting system risk analysis. Whether or not the described threats apply to a specific voting system depends on the implementation details of the system in question. The trees and

proposed controls in our report can facilitate data capture to support systematic risk analysis, but should not be projected onto any operational system without mapping all relative properties of that system in the threat tree. This is precisely the task that the EAC described as their required functional capability. The TIRA environment (MicroSoft Excel) is widely available and is designed to allow analysts to create, copy, and modify voting system threat trees for use with TIRA.

3. This project is not intended to answer all questions about relative risk in voting systems. In fact, the investigators conscientiously avoided rendering such judgments. Rather, the project provides resources to allow the EAC to reach sound decisions relative to voting system standards that include consideration of systematic risk analysis.
4. This project does not evaluate the effectiveness of mitigation strategies/controls. Again, the project intends to facilitate these decisions by the EAC, as they relate to voting system standards.

Let me now shift to a few details about the project process. An essential element of each component of each phase of this project was peer and subject matter expert review. While many of the project artifacts were created by individual team members, the review process was rigorous and at many stages, the requirement to accomplish a thorough review dictated the project pace.

Project deliverables were formally vetted through a four-tier process that included at least one review at each of the following levels:

1. Project Team review.
2. Project Team Advisory Board review.
3. Formal review panel.
4. Review and feedback from the EAC advisory bodies (Standards Board, Board of Advisors, National Institute of Standards and Technology).

In addition to the formal reviews, several artifacts were sent to external reviewers for further comment and the Project Team presented the threat trees and risk assessment tool to the Technical Guidelines Development Committee, receiving substantial feedback during and after that presentation. The project team carefully and systematically analyzed and incorporated comments from the review process into the project artifacts.

On behalf of the Project Team and the University of South Alabama, I offer our deepest thanks and appreciation to the many professionals and experts that volunteered their time on this project. There is no substitute for their valuable contribution and we are indebted to them.

Thank you again for the opportunity to speak. I'll now ask Harold Pardue and LisaAnn Benham from the Project Team to join me and we are happy to take questions.