Testimony of Brian J. Hancock & Matthew Masterson

EAC Public Meeting March 11, 2010

Election Operations Assessment Overview

Introduction

The EAC's Election Operations Assessment ("Assessment") came about as a result of the public comment period for the Next Iteration of the VVSG. In August 2007, the TGDC delivered a set of recommendations for the next version of the Voluntary Voting System Guidelines (VVSG) to the EAC. These recommendations considerably expand the number of security requirements for voting systems. They also introduce several new concepts to be applied in system design and testing. The EAC must decide how to utilize these recommendations as they create the next iteration of the EAC voting system standards. This requires answering the question of how to specify a sufficient level of security protection without requiring disproportionate tradeoffs against other desirable attributes such as ease of use, efficiency of operation, and reasonable cost. At the time the TGDC recommendations were forwarded to the EAC there was no complete analysis of the risks posed to voting systems and the potential resulting harms.

To gather input for its deliberations on the next iteration of the VVSG, EAC convened a series of seven roundtables of all major stakeholder groups to discuss the purposed voting system requirements. One focus point for all of these roundtables was the lack of a definitive risk assessment model for

voting systems, and the necessity of having such an assessment in order to provide a framework for identifying and prioritizing security requirements. This is consistent with federal information security policy in general as well as IT industry security best practices.

As a result of this feedback the EAC conducted a competitive procurement process to obtain the services of an inter-disciplinary team to perform a scientifically based comprehensive Voting System Risk Assessment. The University of South Alabama team, with Dr. Alec Yasinsac as the Principal Investigator, was selected. The results of this effort are expected to assist the EAC in making informed decisions relative to future voting system standards.

The Election Operations Assessment

The assessment project work was laid out in two distinct phases. The first phase created two sets of reference models: 1) election process models to define the operational context in which voting systems are used, and 2) voting system models by generic technology type to identify the variations in threats and potential impacts across the range of voting technologies. The generic voting types analyzed were:

1. Hand counted paper ballots
2. Direct recording devices
3. Precinct Based optical scanners
4. Vote-by-phone
5. Internet voting
6. Vote-by-Mail
7. Central count optical scanners

In the second phase the models were analyzed to identify the risks associated with each voting technology and to perform assessments of the potential harms and possible mitigations for these threats. The end product is a set of risk assessments for the range of voting technology approaches. The intention of this analysis is not to rate one technology as better as or worse than another or to identify the "best" system, but rather to identify the security requirements necessary for all types of systems to achieve a specified level of confidentiality, integrity, and availability. Achieving a mix of all three of these may be technically more difficult for some

technologies and/or expensive and entail undesirable tradeoffs against other important design considerations such as usability.

There were two deliverables for the project's second phase. The first of these was an analysis of the voting system models to identify generic threats associated with each voting technology. This information was captured as a set of threat trees using NIST 800-30 threat definitions, one threat tree for each technology type.

The second Phase II deliverable was the development of a tool to assist the EAC in evaluating the relative harm magnitude of identified threats and to facilitate a cost-benefit analysis on the potential mitigations for those threats. The tool was required to be useable by non-expert users at the EAC without the assistance of technical experts and could not use any restrictive proprietary data formats.

One of the mandated project tasks was to create buy-in from various sections of the elections community on the assessments process and work product. This buy-in was accomplished by having each phase of the assessment peer and subject matter expert reviewed. While many of the project artifacts were created by individual team members, every artifact was vetted through the following levels: the team level, the VSRA Advisory Board level, a formal review panel, and feedback from the EAC's Board of Advisors and Standards Board. The project team and project advisory board members represented a broad spectrum of election and technology expertise with members from many different states, thus ensuring breadth of experience and perspective in the vetting process. Additionally, several project deliverables were sent to external reviewers for further comment.

Conclusion

Over the course of this project the University of South Alabama and the EAC have worked closely together to ensure a work product that is both useful and useable. The assessment tool created by the project team will serve as an valuable resource as the EAC moves forward with the development of the next iteration of the VVSG. EAC staff, in conjunction with the technical experts from the National Institute of Standards and Technology (NIST) will use the tool to conduct in depth cost/benefit analysis of proposed requirements. This analysis will ultimately lead to a standards document that is both rigorous and cost effective.