MEMORANDUM FOR THE RECORD

Subject: Comments on Rule # IS-2.004. Procurement, Use and Assessment of Voting Systems

Thank you for the opportunity to address you. My name is Dr. Alec Yasinsac. I am a retired Marine, local businessman, faculty member at Florida State University, and long time information security researcher. I am commenting regarding the proposed Florida Rule # IS-2.004, specifically regarding its potential impact on voting systems security. I am concerned that the rule, as presently worded, will decrease the opportunity to secure the voting process. The section of Rule # IS-2.004 that I will be referring to is included in the following inset.

> (a)1. The supervisor of elections on his or her own, or upon the direction of the governing body, may conduct an assessment of a voting system for the purpose of examining or evaluating security procedures, access control, system reliability and accuracy. This assessment may be conducted as a routine test or a test on the basis of paragraph (2), a system audit or an examination of the functionality of the software and firmware and may include penetration testing. The supervisor of elections is responsible for the conduct of these assessments but may use the services of an independent professional person or entity approved in writing by the Division. The professional person or entity must possess one or more relevant certifications from either the American Software Testing Qualifications Board (ASTQB), the American Society for Quality (ASQ) or from EC-Council.

My concern is with the final sentence of this passage that limits authorized assessment organizations and persons by requiring assessment organizations be certified through one of three selected programs. The terminology gets a little tricky here. The passage mandates *organization/individual skills certification* for voting system assessors, essentially imposing a reputation or credibility standard. In the following paragraphs, I introduce the certification-related notion of *system verification* and contrast that with *system assessment*.

It is important to emphasize that the subject passage deals with system assessment, not system verification. System verification spans the development lifecycle and targets comprehensive functional analysis, essentially ensuring (possibly certifying) that a system accomplishes its goals. The developer generally performs system/integration testing, traditionally as the development life cycle conclusion. Though newer lifecycle models have less synchrony, in virtually all models, the developer exclusively accomplishes system testing and it is almost without exception time-driven. Verification commonly culminates in beta testing to identify

errors that may occur "in the wild" but that are difficult to identify in standard testing methodologies.

Conversely, system assessment targets finding problems, flaws, vulnerability, and exposure to malicious acts. This process is often domain specific, i.e., specific application area knowledge enhances assessment, as does operational experience. It is not unlikely that two different, equally qualified assessment organizations, given the same period of access, would produce radically different assessment results, and that those results could be of equal quality. System assessment leverages some scientific method, but is largely an art.

Another important distinction between assessment and verification is that, unlike verification results, assessment results are easy to confirm. While system verification targets comprehensive analysis, it is well known that verification only reflects that tested processes work correctly and that certain errors were not found, not that ALL functions are correct nor that no errors exist. Corroborating a comprehensive verification would require a separate, comprehensive, lifecycle wide verification process occur (called Comparison Testing). Conversely, when assessments identify specific problems, we can easily reconstruct the tests, demonstrate the vulnerability, and document and confirm, or refute, the assessment results.

I make the distinction between system verification and system assessment because requiring certification for verifiers provides significant value, while certifying assessors is likely counter-productive. Finding problems often demands non-monolithic approaches from investigators with varying skills and perspectives. Assessor certifications tend to bound problem verification techniques into classes and to funnel thought processes into specific frameworks. This is contrary to the "out of the box" mentality necessary for effective assessment. There are many assessment techniques and approaches and certification cannot be comprehensive and is rarely broad.

The subject rule passage above acknowledges that SoEs are in a unique position to identify potential voting problems and vulnerability and that they need sufficient latitude to formally investigate potential problems. Unfortunately, the rule's final sentence unnecessarily constricts this latitude. From a security standpoint, an assessment that finds no errors is a benign event, one that finds a verified flaw is an unequivocal success, and the two are easy to distinguish.

Conversely, while ASTQB, ASQ, and EC-Council offer software quality, testing, and security certifications, there is no data that correlates their certification(s) with secure voting systems. On the other hand, members of security centers, such as the ACCURATE (A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections) at Johns Hopkins University, could provide broad security skills and extensive domain experience. It is unlikely that such centers will consider ASQ, etc. certification. Similarily, many of the world's premier security consultants base their credibility on documented procedures, performance, and success. Counterpane, Inc. is one example. Their web page[1] reflects a commitment to success with their track record being the cornerstone of their reputation and the foundation for winning customer trust. Such consultants do not need and will not seek ASQ, etc. certification. Thus, it is likely that the arbitrary rule limitation would disqualify the most qualified assessment resources from service.

Sound security policy should embrace anyone that can find flaws, as long as the flaws can be easily verified/contradicted, which has proven to be true so far in this debate. It is widely recognized among software and security specialists that the more open and varied the assessment, the more likely that system flaws can be identified and removed.

For these reasons, it is likely that the requirement as it is written will reduce voting system software security. I am well aware that vendors are sensitive to assessment techniques and that they have a vested interest in the process. It is in everyone's best interest if qualified, dedicated vendors offer their services to Florida voters. However, limiting access in any form is a double-edged sword. While centralizing or monopolizing control, it also expands vulnerability impact. In cyber-jargon, this is termed the "shrink wrap" effect. If a flaw exists and is exploited in the monopolized system, broad impact is ensured by policy.

It is my strong opinion that security should be the overriding priority in this rule. There is value in identifying specific criteria, e.g. certifications that can unilaterally qualify assessment organizations and can help SoEs select suitable assessors. The exclusivity creates the security problem, preventing SoEs from selecting the best assessor for the job.

[1] http://www.counterpane.com/wins-trust.html

Fortunately, there are several simple options to reverse the rule's present negative impact. The ideas below have some complementary properties and are not mutually exclusive.

(1) Allow SoEs to engage any assessment team. This allows the greatest flexibility and provides the best opportunity to identify voting system vulnerability.

(2) Introduce an escape clause to allow SoEs to engage skill-appropriate assessment teams based on documentary credentials approved by the governing body.

(3) Appoint a software or security Center of Excellence or other independent organization or consortium to approve exceptions to the certification requirement.

(4) Adopt and publish a simple process to add certification organizations to the already established list of three.

Again, thank you for your time and attention. I will gladly take questions if any exist.