FVAP Statement on Research Reports Related to UOCAVA System Testing

Scope and Purpose

In 2010, the Federal Voting Assistance Program (FVAP) sponsored research on the *Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA)* Pilot Program Testing Requirements (UPPTR) as adopted by the United States Election Assistance Commission (EAC). This research intended to inform the project planning and execution of the Department of Defense's legislatively mandated electronic voting demonstration (i.e., remote electronic voting) requirement, first established in the National Defense Authorization Act of 2002. In 2015, Congress eliminated this requirement; however, the resulting reports from the commissioned research remained unpublished at the time of the repeal.

In order to consider the future direction and voting system architecture surrounding a remote electronic voting system or the consideration of future pilot programs, FVAP's 2010 research objectives were 1) assess the current UPPTR as conformance standards for use by FVAP when fielding a specific voting system (i.e., electronic voting kiosk), and 2) assess the extent that the requirements would need additional security standards for a Department of Defense sponsored electronic voting solution. Although Section five of the UPPTR explores the use of penetration testing in conformance testing, FVAP's consideration of a remote electronic voting solution led to the development of a proof-of-concept approach for additional penetration testing as part of an eventual project implementation.

FVAP had four objectives for these studies: (1) evaluate portions of UPPTR that would apply to information assurance for sufficiency and clarity; (2) evaluate the value and impacts of an FVAP sponsored certification/conformance test to the UPPTR; (3) evaluate the subjective differences between the different voting system test laboratories to inform FVAP project planning; and (4) establish a viable proof-of-concept for future penetration testing as part of FVAP's overall information assurance posture.

These reports were originally intended to foster an ongoing discussion as part of the standards development process in partnership with the EAC and National Institute of Standards and Technology (NIST). As of June 2012, all mechanisms for future discussions dissolved due to changes in FVAP leadership and the lack of EAC Commissioners. Without the supporting federal advisory committees to guide the process, FVAP relied on these reports to inform its possible implementation of future pilots and the electronic voting demonstration project. These reports do not reflect the views and policies of the Department of Defense or FVAP on the concept of internet voting or its ultimate consideration of its efforts to complete the electronic voting demonstration requirement. FVAP anticipates releasing additional research by the end of 2015.

No other conclusions should be drawn beyond the findings stated in the reports and any resulting analysis should be done so in recognition of the following limitations:

Limitations on Voting System Laboratory Testing (VSTL) Report

- Vendors did not submit source code or technical data packages and no code review was performed. There was no opportunity for remediation.

- Indications of pass/fail in the test results do not indicate how well a particular system would perform during a full certification test and may be the result of test interpretation or applicability.

- No systems were presented for certification and certification was not a potential outcome. Only a small portion of the complete UPPTR was studied. Sections two and five of the UPPTR were evaluated and the remaining eight sections were not evaluated.

- The formal EAC process for voting system certification was not followed. Manufacturers are normally allowed to remediate any deficiencies found and submit the system for retesting. For this study, there was no interaction between the EAC, the manufacturer, and the Voting System Testing Laboratory. Each system was evaluated once, in a limited fashion, and the results documented.

Limitations on Penetration Test Model Design and Methodology

- These tests were only intended to serve as a proof-of-concept for the establishment of a model design and methodology for future penetration testing.

- The manufacturer names are not disclosed. The purpose behind these tests was not to evaluate any specific system, but to evaluate the requirements and the process.

- The penetration test period was limited to 72 hours, a significant limitation from expected real world conditions.

- Certain types of attacks, such as Distributed Denial of Service, social engineering, and physical tampering were not allowed. Since the time of this research, the attack profiles and methodologies have significantly changed, thus these tests should be viewed only within the context of when they were conducted.

Conclusions

FVAP found opportunities for improvement in sections two and five of the UPPTR, the core areas of focus in this research. If this research followed a full certification protocol as outlined in the EAC certification program requirements, those ambiguities identified would likely be resolved through a structured test plan and the Request for Interpretation process.

The test results from the different labs were presented in widely different formats. FVAP recommends standardization of test lab reports so relevant stakeholders can benefit from findings that do not reflect the individual styles of each test lab.

Although much of the UPPTR could be applied to remote electronic voting systems, a detailed review would be necessary to determine which requirements apply to these systems directly.

The penetration testing model revealed issues that must be addressed prior to its usage in an accreditation environment. Future consideration of penetration testing must clearly identify the requisite skills and experience of testers to ensure high confidence in the results. The penetration test methodology used during this proof-of-concept exercise also highlighted the difficulties of testing these systems in a realistic environment. Testing across public networks in such a way as to not interfere with other uses was difficult and limiting.

Expanded efforts to develop more robust penetration testing for systems used by *UOCAVA* voters should not use passive tests to assess how products perform, but should instead assess the overall ability for the supporting networks to detect and respond to threats and attacks. Penetration testing should be an ongoing process, conducted in an actively monitored environment, to determine how system operators can respond to potential intrusions.

Recommendations

With the passage of the 2015 National Defense Authorization Act and the repeal of FVAP's requirement for the conduct of an electronic voting demonstration project (i.e., remote electronic voting), the Department of Defense is no longer exploring program implementation in this area and these reports should not be used to convey a position in support of States to move forward with such technology. However, both of these reports mention a series of recommendations which may prove instructive. FVAP will work with the EAC and NIST through the standards development process provided under the *Help America Vote Act* to consider the following:

1. Integration of the individual report findings and recommendations into the consideration of future voting system standards.

2. Exploration into the viability of incorporating structured penetration testing for *UOCAVA*-related systems and qualifications for penetration testers.