

## **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 In 2015, Congress eliminated this requirement; however, the resulting reports from the commissioned research remained unpublished at the time of the repeal.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.



# Federal Voting Assistance Program (FVAP) Penetration Testing of a Simulated Election

*16 September 2011*





# **Penetration Test of Simulated Election**

---

**Delivery Order # DO 80047-0037**

**Task Order # 5.1.3**

**Final Report**

**Version 1**

**16 September 2011**

## Executive Summary

The Federal Voting Assistance Program (FVAP) has been mandated to carry out a remote electronic voting demonstration project in which a significant number of uniformed service members could cast ballots in a regularly scheduled election. To address security issues associated with such a project, FVAP collaborated with RedPhone Corporation (RedPhone), a professional information security company and the U.S. Air Force Institute of Technology (AFIT) to carry out penetration testing of three electronic voting systems.

Penetration testing, or PenTesting, is an integral form of security testing which challenges online system security using techniques similar to those used by criminals and other hostile entities intent on inflicting genuine harm. However, in an authorized PenTest, all parties agree to the testing; and the testing is conducted for the benefit, not the harm, of the system vendors and all stakeholders. The findings of the PenTest are evaluated so that mitigation strategies can be developed and applied to manage security risks to acceptable levels.

The PenTest was conducted in August 2011 using online voting systems developed by three major online voting system vendors (who will remain anonymous in this report), whose systems are successfully used by jurisdictions throughout the world to conduct online elections. The intent of this PenTest and subsequent analysis was to provide the FVAP Director with usable information about the security posture of current online voting systems, and to provide data that supports decisions regarding FVAP's future Congressionally-mandated demonstration project. This document presents the findings and recommendations of this PenTest as well as suggestions for future work in this realm.

The most notable overall finding of the PenTest was that none of the vendors' systems were compromised. Neither RedPhone nor AFIT were able to penetrate or exploit the three online voting systems during this testing exercise. Additionally, all evaluated online voting systems passed all of the Penetration Testing requirements enumerated in the Security section of the UOCAVA Pilot Program Testing Requirements (UPPTR). Despite the systems passing this testing, AFIT and RedPhone found areas that each vendor should address to ensure that their systems are as secure as possible. Specific recommendations include:

- improving technical security;
- hardening physical security;
- building a cooperative security relationship;
- assigning security responsibility between the servers and the remote voting stations;
- including personnel training, system certification, and continuous security monitoring from government and industry best practices and guidance;
- undertaking periodic PenTests and other security tests in the future with concurrent development of test cases and requirements; and
- developing operational PenTests during iterative pilot projects conducted in CONUS, OCONUS, Ship Board and Hostile environments, which are intended to lead to the Congressionally-mandated FVAP demonstration project.

## Table of Contents

Executive Summary .....	iii
1 Introduction.....	5
1.1 Why Penetration Testing Was Done .....	5
1.2 Impact of Results.....	7
1.3 Evolution of the Penetration Test.....	7
1.4 The Stakeholders Involved.....	8
1.5 The Penetration Teams.....	8
1.6 The Process .....	9
2 Test Development and Participants.....	10
3 Methodology .....	14
4 Results.....	17
5 Recommendations.....	25
6 Conclusion .....	29
Appendix A: AFIT Report.....	30
Appendix B: RedPhone Report.....	31
Appendix C: Security Gap Analysis of UOCAVA Pilot Program Testing Requirements .....	32

# 1 Introduction

## 1.1 Why Penetration Testing Was Done

Perhaps the most cherished right American citizens have is to govern themselves by electing leaders through the voting process. Unarguably, no one is more entitled to this right than the men and women of the United States military who commit themselves to defending this right. Yet, many of military service members, their dependents, and other qualified voters are located throughout the world in places that make it impossible for them to physically report to a polling place to cast their ballot. To accommodate these individuals, a paper-based, absentee voting process is currently utilized by military voters, their dependents, and other overseas voters.

The Federal Voting Assistance Program (FVAP) is exploring the use of current electronic technologies to provide authorized military voters with online voting capability through an electronic network. Meanwhile, election jurisdictions in the U.S. have undertaken their own online voting pilot projects by experimenting with secure electronic ballot delivery, using email/fax/U.S. Postal Service to return marked ballots. The jurisdictions focused on convenience issues, the potential for increased turnout, and the opportunity to streamline the UOCAVA voter absentee voting process to ensure ballots are delivered to their respective voting jurisdictions accurately and in sufficient time to ensure that these absentee ballots are counted.

There are security issues inherent in any electronic or online voting system, just as there are security issues with the current paper-based absentee voting process. Online voting security issues must be individually and collectively addressed in order for online voting to be an acceptable alternative to the current paper-based process. The goal is not perfect security, since perfect security is, and will always be, impossible to attain. Therefore, the standard to reach is security that is at an appropriate level, or provides a high level of assurance. The decision to use online voting involves a balance between the security risks and the benefits to be derived.

One way to measure and improve online voting security is to conduct security testing for systems that are currently available and in use. One such security test is called Penetration Testing, or PenTesting. PenTesting involves attempts to challenge the security capabilities of the system in question. A PenTest is conducted by individuals appropriately trained, experienced, and authorized in this discipline. PenTesting is both an art and a science, and it uses a variety of techniques, including technical, administrative, personnel, physical, and all other methods that can “break” a system. It uses techniques similar to those used by unscrupulous criminals who are intent on inflicting genuine harm to a system. The difference in an authorized PenTest is that all parties agree to the testing, and the test is conducted for the benefit, not the harm, of the system vendors and all stakeholders.

PenTests are conducted according to strict Rules of Engagement, and they include well-defined legal permissions. PenTest results can expose system weaknesses or vulnerabilities that match specific threats—threats that would be posed by malicious sources. The results of a genuine, successful attack by a malicious source can have negative system consequences or impacts, and these factors result in a risk



level (high, medium, low) to the system. The PenTest is designed to simulate a “real” attack to expose vulnerabilities to particular threats, and to provide intelligence that can be used to improve security.

The PenTest findings can be evaluated; and mitigation strategies can be developed and applied to control and reduce risks to acceptable levels. Controls take the form of safeguards and countermeasures designed to prevent, detect, and correct problems; thus reducing security risks to acceptable levels. This process, in theory, “hardens” the system against potential true attackers in a live environment.

During August 2011, a PenTest was performed to expose security risks for online voting based on three products offered in the marketplace. The systems subjected to the PenTest were three companies currently providing online voting capabilities throughout the world. To protect their privacy, in this report, these companies are referred to as Vendor-1, Vendor-2, and Vendor-3. These vendors agreed to participate in a PenTest as a way to improve their system security, with the goal of providing secure online voting capabilities to authorized individuals.

Two organizations conducted the PenTest on the cooperating vendors’ systems. One of these organizations, RedPhone ([www.redphonecorporation.com](http://www.redphonecorporation.com)), is an experienced information security company. RedPhone is located in the Washington, DC area and specializes in PenTesting and other information security protocols for a wide variety of clients including multinational corporations, the U.S. Air Force, U.S. Army, U.S. Army National Guard, U.S. Navy, U.S. Marine Corps, U.S. Coast Guard, U.S. Customs, Bureau of Alcohol, Tobacco and Firearms, the Department of Justice, and the U.S. Navy Criminal Investigative Service.

The second organization that conducted PenTesting as part of this project was the U.S. Air Force Institute of Technology (AFIT) located at Wright-Patterson Air Force Base in Dayton, Ohio ([www.afit.edu](http://www.afit.edu)). PenTesters in the AFIT organization consisted of highly motivated, well-educated, ROTC college engineering and computer science students on a summer educational internship. The students were participants in the ACE (Academic Center of Excellence) Cyber Security Boot Camp Program. This program is held each summer for a select group of ROTC students studying computer science or cyber security. The curriculum consists of cyber warfare, digital forensics, cryptography, reverse engineering of software and many other subjects. The boot camp lasts for eight weeks and culminates in “Hack Fest.” During Hack Fest, the students participate in various exercises where they conduct cyber-attacks, defend against a cyber-attack, and plan attribution strategies. The students were mentored by some of the most skilled experts in the field of cyber security, all having earned their PhDs in cyber security or computer science. These highly trained professionals have direct access to the most modern facilities and equipment in the world.

The mix of PenTesters (the juxtaposition of the professional experts at RedPhone and the academic college students) provided the wisdom and experience of a professional company with the creative ideas and approaches of youthful, competitive, highly skilled and highly motivated military college engineering students, mirroring in many ways the attributes of youthful hackers in the threat environment.

This report provides the results of these two PenTests. Appendix A is the report from the AFIT students and Appendix B provides the report from RedPhone. Appendix C is a Security Gap Analysis of the

UOCAVA Pilot Program Testing Requirements that was conducted by RedPhone for FVAP in February 2011, before the commencement of the PenTest project. The AFIT students' report at Appendix A gives a high-level view of the findings, vulnerabilities, impacts, and recommendations for improvement, while the RedPhone report at Appendix B gives a more detailed, "bit-level" technical evaluation of the vendors' security risks. Both reports have been reviewed and all proprietary information has been removed; however, each vendor did receive a report specific to its own company that can be used to improve system security.

Chapters 2 and 3 of this paper summarize the findings and recommendations, but leave the details to the Appendices, which were written by the individual groups who conducted the actual tests.

## **1.2 Impact of Results**

The results from these two PenTests will inform all online voting system vendors and stakeholders of security vulnerabilities, threats, impacts, and risks, and provide recommended controls (safeguards and countermeasures designed to prevent against, detect, and protect assets), thereby implementing mitigation strategies to reduce the risks associated with online voting to acceptable levels. This research may also assist with general recommendations to the U.S. Election Assistance Commission in the adoption of voting system standards and relevant security standards for internet voting.

## **1.3 Evolution of the Penetration Test**

The 2002 National Defense Authorization Act (NDAA) and the Military and Overseas Voter Empowerment (MOVE) Act of 2009 significantly expanded the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) of 1986, which protects the right of service members to vote in federal elections regardless of where they are stationed and calls for the establishment of a demonstration project to test electronic voting for absentee uniformed services voters in a federal election.

Security of online voting systems has been the subject of much conversation among voting technology providers, academics, and those concerned with online voting security. FVAP has so far conducted three UOCAVA Solutions Working Group (USWG) meetings over the past two years (2010-2011), with the main discussion topic being the security of online voting systems. The need for data providing security information about these systems was the genesis of the PenTesting effort. The NDAA requires consideration of the national level threat. As such, FVAP has engaged in this direct effort to learn the current level of security as established currently in fielded/available systems for procurement.

There have been other types of electronic voting systems (for in-polling place use) subjected to certification testing through the EAC and or various state certification programs that have included a minimum amount of PenTesting, but not on the scale that has been done through this effort and this has not included PenTesting of online voting systems. The FVAP PenTest is of a much larger scope and included three online voting systems that are widely used worldwide. The intent of the PenTest was to provide the FVAP Director usable information about the online voting systems' security posture, and provide data that supports decisions on the electronic voting system way ahead that FVAP must develop and execute.

## **1.4 The Stakeholders Involved**

FVAP could not do this testing alone. Several organizations and commercial enterprises were involved in executing this project. The FVAP Director desired to have as much participation from the voting system vendors as possible, and the three major vendors in particular. The project required setting up voting stations for each vendor's system to allow volunteer voters to cast their ballots. The space for the voting stations required an acceptable level of privacy, yet easy access for the volunteers. Technical expertise was required to set up these systems and to provide the required network connectivity. There also was a need for technical expertise to plan how to best attempt to breach the security of the voting systems.

AFIT volunteered their assistance in this experiment and provided the laboratory space for the "hackers" to use, space for the voting systems and volunteer voters, and specially trained students to serve as one set of "malicious" sources. AFIT also provided all network connectivity needed for the voting systems, the Internet Protocol (IP) addresses needed for the experiment and all of the "hacking" software used in the PenTest including COTS (commercial off the shelf), open source and proprietary tools.

Professional cyber attacking experience is also a critical part of any exercise like this and RedPhone provided all the technical expertise needed in this area. The curriculum at AFIT did not cover cyber hacking to the degree necessary to execute a successful penetration attempt. Therefore, additional training on cyber-attacks was provided to attempt a penetration attack on their voting systems. The vendors' names will not be used in this jointly by FVAP, RedPhone and Mr. John Rossi, a recently retired government employee who taught cyber security to federal employees. The training was comprehensive and laid a firm foundation for the students of AFIT to design and execute their attack plan.

AFIT was a superb venue for the PenTest. The staff was very helpful and cooperative and had a real interest in this project. The PenTesting was mutually beneficial to both AFIT and to FVAP. AFIT enhanced student skills and FVAP gathered useful data about online voting system security. AFIT also expressed interest in working with FVAP on future projects in this area.

None of this would have been possible without the cooperation of the three voting system vendors whose openness and cooperation was key to a successful PenTesting effort that provided much usable data.

## **1.5 The Penetration Teams**

RedPhone is a high profile information security company that provides cyber audits to the federal government, local government and to commercial enterprises. RedPhone developed the cyber security test plan that outlined what specifically the penetration attempts would do and what they would not do. RedPhone also provided one two-person team that performed the PenTest over the 72-hour test period. The AFIT students were also active participants in the PenTesting. The students formed two three-person teams that worked to penetrate the voting systems concurrently with RedPhone.

## **1.6 The Process**

The PenTest was successful due to the cooperation of all the stakeholders. The next step may be to hold a mock election for a local election jurisdiction or for an organization. While the actual voting is being conducted, “hackers” could be attempting to enter and alter the votes being cast. Another option may be to have a “mock” election and have voters from several different locations participating in the election. This would distribute the voters in what would be a more normal pattern. The “hackers” also would need to be more skilled to fully test voting system vulnerabilities. Many different scenarios could be developed to provide even more detailed data on electronic voting security. The bottom line is that FVAP should not stop here, but forge ahead to collect as much data as possible to improve the decision making process for the mandated demonstration project.

## 2 Test Development and Participants

Multiple vendors were invited to participate in the mock election scenario exercise held at AFIT. Ultimately, three were chosen and participated, agreeing to allow AFIT students and industry professional PenTesters to attempt to breach the security of their remote Internet-based voting systems. Mutual Non-disclosure Agreements (MNDA) and Rules of Engagement were signed by all parties and participants in the PenTesting to ensure that appropriate boundaries were defined. The AFIT students and RedPhone PenTesters were not permitted to use social engineering methods or to interfere with corporate IT systems; only those servers and voting stations used in the mock election exercise were targeted.

RedPhone fully understood the requirements as outlined in the UOCAVA Pilot Program Testing Requirements (UPPTR) for security testing and identified the following requirements as essential:

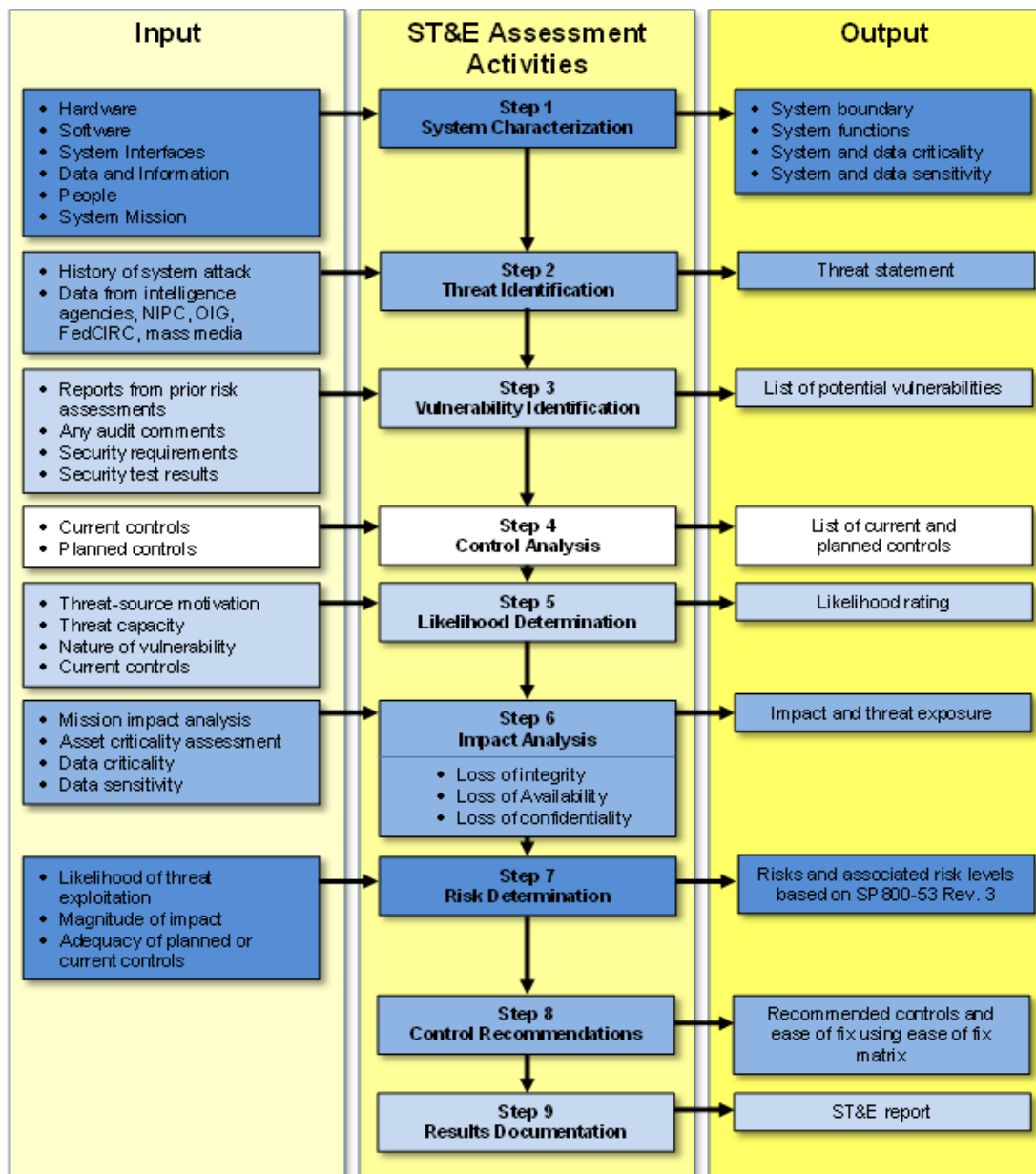
1. Security test results must be documented and formatted in a way that conveys information to FVAP that can feed the internal risk management processes.
2. Security test reports must contain information sufficient for senior leadership to make informed, risk-based decisions.
3. Experienced tactical information security teams will be required to meet the schedule.
4. Formal project management techniques will be needed for PenTest coordination across multiple locations simultaneously.

RedPhone's approach was based on the National Institute of Standards & Technology (NIST) Special Publication 800-53 rev. 3 and Federal Information Security Management Act (FISMA) requirements. It also leveraged the National Security Agency Information Assurance Methodology (NSA-IAM/IEM) and the Information Systems Security Assessment Framework (ISSAF) approach often used by federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels.

The Security Test and Evaluation (ST&E) process directly supports security accreditation by evaluating the security controls in the information system. This evaluation is conducted to determine the effectiveness of those security controls in a particular environment of operation and the vulnerabilities in the information system after the implementation of such controls. The ST&E can include a variety of verification techniques and procedures to demonstrate the effectiveness of the security controls in the information system. These techniques and procedures can include such activities as observations, interviews, exercises, functional testing, PenTesting, regression testing, system design analysis, and test coverage analysis. The level of rigor applied during evaluation is based on the robustness of the security controls employed in the information system—where robustness is defined by the strength of the security controls and the assurance that the controls are effective in their operation. Authorizing officials and their designated representatives are better positioned to make residual risk determinations and the ultimate decisions on the acceptability of such risk after reviewing the results of such evaluations.

ST&E should not be viewed as a static process. An information system is authorized for operation at a specific point in time reflecting the current security state of the system. However, the inevitable changes to the hardware, firmware, and software in the information system, and the potential impact those changes may have on the security of that system, require a more dynamic process—a process capable of monitoring the ongoing effectiveness of the security controls in the information system. Thus, the initial security accreditation of the information system must be supplemented and reinforced by a structured and disciplined process involving: (1) the continuous monitoring of the security controls in the system; and (2) the continuous reporting of the security state of the system to appropriate agency officials.

RedPhone recognizes that detecting vulnerabilities is a specialized security function within the information technology field. Therefore, they developed small, highly skilled teams specifically trained for federal ST&E support. These information assurance Tiger Teams consisting of one Tactical Team Leader, one or more PenTesters, an audit and policy analyst, and one system engineer. Their functions and roles vary depending on the size and scope of the engagement. The purpose of these teams is to use a systematic approach to identifying and reporting vulnerabilities. RedPhone uses the process outlined in Figure 1 below to support penetration testing efforts.



**Figure 1. RedPhone Security Test and Evaluation Process**

Identifying risk for an IT system requires a keen understanding of the system’s processing environment. The ST&E team must therefore collect system-related information first, which is usually classified as follows:

1. Hardware
2. Software
3. Port, protocols and services being used
4. System interfaces (e.g., internal and external connectivity)
5. Data type and classification
6. Persons who support and use the IT system

7. System mission (e.g., the processes performed by the IT system)
8. System and data criticality (e.g., the system's value or importance to an organization)
9. System and data sensitivity

Use of Automated Scanning Tools and other proactive technical methods were used to collect system information efficiently. For example, network mapping tools were used to identify the services that run on a large group of hosts and provide a quick way of building individual profiles of the target IT system(s). RedPhone used at a minimum Nessus, NMAP, and Metasploit for PenTests.



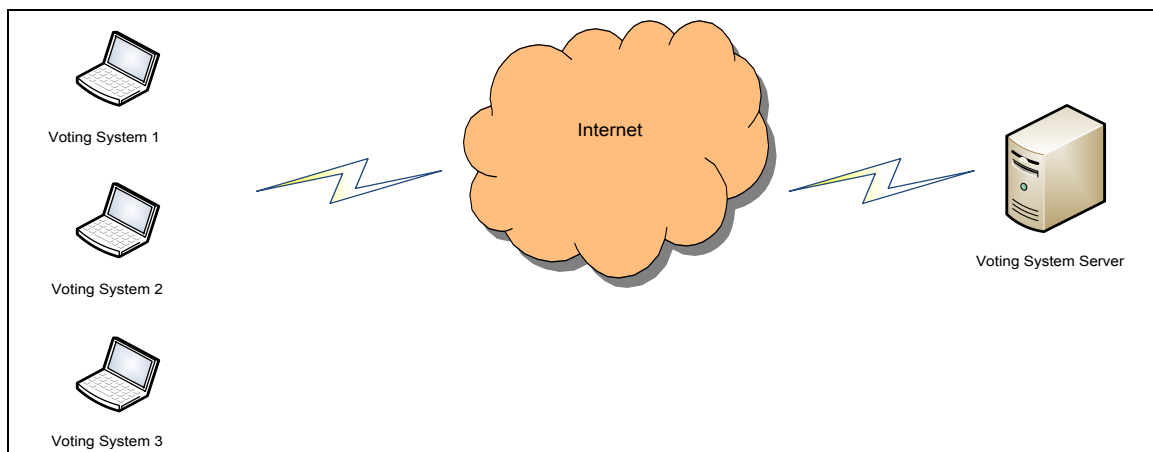
### 3 Methodology

The following text describes the methodology used to conduct the PenTest and outlines how the experiment was designed, the test environment, the teams involved in the test, and how ballots were cast. Also outlined is what was *not* undertaken for this mock election PenTest.

The AFIT students received training from Mr. Rossi on network security concepts. They also received three separate PenTesting training sessions provided by the RedPhone team. This training provided the students with actionable knowledge on how to construct a test plan, execute the plan, and properly format and report the team’s findings. Additionally, the students were provided hands-on training using many “hacker” tools. Examples of these tools include Metasploit, Nessus and NMAP. Each training session provided a logical information progression on each vendor, the tools (and how to use them), and how to build a successful PenTest. The AFIT students also were provided templates for constructing their test plan and the final report format for their findings. The graphic in Figure 3 provides a step-by-step explanation of how the voter cast a ballot and at what point the PenTest teams attempted to penetrate the systems.

A student lounge used by AFIT students served as the polling place for the mock election portion of the PenTest. This area was selected because it was easily accessible by the AFIT students, and they were frequently in the area during breaks and lunch. Since the students were the volunteer voters for the experiment, it was essential that an area be provided that was convenient for them to access. AFIT provided each vendor one laptop computer with only the operating system, Internet Explorer and Firefox installed. The voting computers were inserted into the AFIT network, but were provided Internet access without going through any firewalls or other security devices. Figure 2 below, graphically depicts the AFIT test system environment.

**Figure 2. Depiction of Voting Computers used at AFIT**

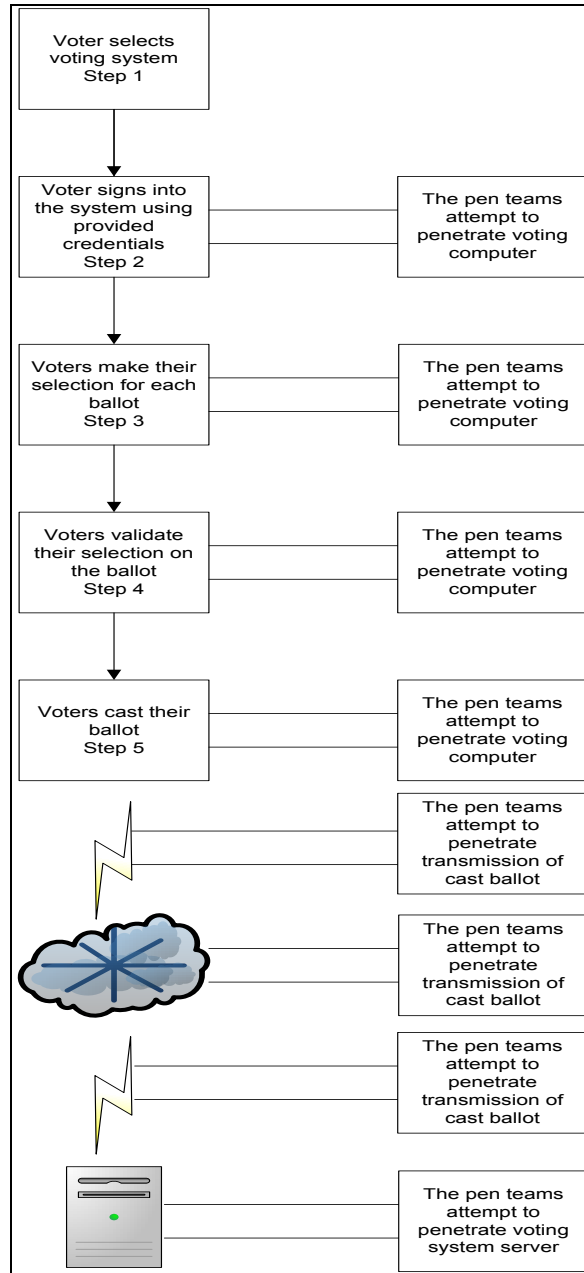


AFIT assigned each computer a static IP address and these IP addresses were given to each hacking team. The systems were left operational for the entire 72-hour period. The student lounge was accessible by the volunteer voters at any time to cast their ballots; however, traffic through the lounge did abate after

normal duty hours, which are 0730–1700 Monday through Friday. Although the AFIT facility is located on a secure military installation, there were no specific physical security precautions taken to protect the machines; no locks or security cables were used to secure the systems to the shelf; and no guards posted to protect the voting machines. The systems did not time out nor did they allow a screen saver to pop up after a certain amount of time.

The volunteer voters walked up to the system of their choice—most voted on all three—and cast their ballots. The three vendors supplied any necessary logon credentials, and the voters used these credentials to access each vendor’s Internet voting site. These credentials varied from vendor to vendor, were not complicated, easily used, and allowed the voter to logon to each system’s home page. Each vendor’s system had a different way to cast an online ballot, but the systems were all intuitive and clear instructions were provided on the screen. Each vendor was given one ballot to load into their system. Every voter had the opportunity to vote on each ballot, and voters were prompted if they had under voted or over voted on a particular ballot. Two of the races on the ballot allowed the choice of a single candidate. One race allowed for the voter to pick up to three of six possible candidates.

Both the AFIT student and the RedPhone penetration teams had direct access to each voting computer, and they did approach each machine and cast ballots. The RedPhone team worked mostly off site, but they did approach the machines in the student lounge and cast ballots. As this was a cooperative test, both the AFIT and RedPhone PenTest teams were provided voting computer and voting system server IP addresses. This allowed more time for penetrating the voting systems without necessarily jeopardizing other AFIT production systems.



**Figure 3. Voter Actions and Penetration Attempts**

The PenTest teams were actively attempting to enter the vendor online voting system to change, alter or delete a vote, or votes, beginning at Step 2 and continuing until after the ballot reached the voting system server. These servers were not physically located at AFIT, but were geographically dispersed, with one server located outside the continental United States. Similar to the voting computers, the IP addresses of the voting systems servers were also provided to the penetration testing teams.

## 4 Results

The PenTest findings included technical, administrative, personnel, and physical vulnerabilities of the online voting systems tested. The table below lists each finding, the importance of each finding, and associated recommendations related to each finding. In general, these findings indicate the presence of system vulnerabilities. These vulnerabilities can be exploited by threats and result in impacts/consequences to system confidentiality, integrity, and availability. Each finding must be addressed; the risks mitigated, accepted or transferred, and the security posture maintained over the life of the voting system in order to remain within acceptable levels.

It is important to note that all vendor systems did not present all of these vulnerabilities. Additionally, some of the vulnerabilities listed below are not vulnerabilities specific to online voting systems, but can be present in polling place voting systems or paper ballot absentee voting systems (i.e. “shoulder surfing”). Also, vulnerabilities associated with access to remote voting machines and kiosk supervision/security could potentially have been addressed by the voting system vendors, but client computer security was not under the control of the vendors and was not part of this official test scenario. Even so, with three days of unrestricted access to the voting stations, the attackers were unable to use this advantage to compromise any aspect of the voting process.

**Table 1. Finding/Importance/Recommendation**

Finding	Importance	Recommendation
Open Secure Shell (SSH login) was evident.	Anyone having the correct IP address can access the system, whether authorized or not. The login was protected by userid/password, but these can be hacked by a variety of methods. A successful attack can give a hacker control over the vendor’s server.  The testers were unable to exploit this weakness given the limited time of the test coupled with the requirement to test a variety of weaknesses.	Build stronger authentication. Use either 2-factor (e.g., password and token, smartcard, etc., and/or biometric reader), or strengthen password restrictions such as require upper and lower case alpha characters, require numerals, special characters, etc., and change passwords frequently. Minimize user rights. Follow the recommendation of the U.S. Computer Emergency Response Team (US-CERT) regarding the use of CTR (counter) Mode Encryption.
Testers discovered vendor server information using common hacker tools.	Hackers can use this information to exploit known (or discovered) vulnerabilities, narrow their attack tool choice to focus on the specific vendor system, and use in a social engineering attack. This is a first step in hacking into a system. Once the hack is successful, the system is subject to degraded confidentiality, integrity, and availability.	Use software scanning tools to limit information accessibility; use deception if possible.
Testers breached physical security at the voting	Testers created their own administrator accounts, giving them inappropriate access to	Assign remote terminal security responsibility to the jurisdiction conducting the election. Provide user security training and security

terminal and had easy access to the terminals.	the system and to other voters' activities. Testers were also able to "shoulder surf" other users to obtain sensitive information.	awareness.
SQL injection was able to be performed.	Hackers overflow legitimate computer memory areas and interfere with computer logic and other areas "off limits" to users. This capability puts control into the hands of unauthorized hackers.	Disallow users from entering free-flowing input in database queries. Use prepared statements to limit what a user can enter. Limit the character number and types a user may enter. This limits user control and keeps control with the vendor and the vendor software. This also may assist in mitigating the cross-site scripting vulnerability by controlling user input.
There was use of an SSL cookie.	The application issued a cookie without the secure flag set; therefore, users are not protected from cookies transmitted in unencrypted connections—the cookie is transmitted in clear-text and can be intercepted by hackers.	Set secure flag to prevent transmitting unencrypted cookies.
Script files were unprotected from downloading.	This vulnerability allows hackers to map the site's functionality and expose potential vulnerabilities ripe for attack.	Prevent unauthorized users from downloading scripted files.

Event logging records application, security, and system events for correlation and forensic analysis. Event logging can occur at several places including firewalls, intrusion detection systems, routers and servers, and at the application level. With the event logs, RedPhone obtained information about system hardware, software, and system components, and most importantly security events on both the local and remote servers during the penetration testing. Computers typically record events in the following three logs:

**1. Application log**

The application log contains events logged by programs. For example, a database program may record a file error in the application log. Events that are written to the application log are determined by the developers of the software program.

**2. Security log**

The security log records events such as valid and invalid logon attempts, as well as events related to resource use, such as the creating, opening, or deleting of files. For example, when logon auditing is enabled, an event is recorded in the security log each time a user attempts to log on to the computer. You must be logged on as Administrator or as a member of the Administrator group in order to turn on, use, and specify which events are recorded in the security log.

### **3. System log**

The system log contains events logged by the system components. For example, if a driver fails to load during startup, an event is recorded in the system log.

During the mock election PenTesting exercise, RedPhone maintained communication with each of the vendors and their managed security service providers to determine the speed at which events were triaged, communicated, escalated based on severity, and the accuracy of the logging data. Specific information was recorded, including attacking source IP addresses, time, and date. Throughout the penetration test window, accurate and timely responses from all three vendors participating in the PenTest were provided. Attack events were captured, noted, and escalated quickly with a high degree of accuracy.

Voting systems today face a threat landscape that involves stealthy, targeted, and financially motivated attacks that exploit vulnerabilities at both ends and the middle of the communications process. Many of these sophisticated threats can evade traditional security solutions, leaving voting systems vulnerable to data theft and manipulation, disruption of services, and have the potential to irreparably damage the integrity of the voting process. A review of the UOCAVA Pilot Program Testing Requirements (UPPTR), the Security Gap Analysis found in Appendix C, and the findings from the mock election PenTest exercise held during August 2011 confirmed our suspicions regarding the current threat landscape.

In summary, the Security Gap Analysis prepared by RedPhone and located in Appendix C of this report, found a total of 248 requirements that were identified in the UPPTR document from August 2008 and 2010. While many are functional requirements, all were evaluated by RedPhone for their security risk and potential exploit impacts. Risks were rated as low, medium and high relative to confidentiality, integrity and availability. A security crosswalk was used to map the UPPTR to multiple industry and federal government security best practices and mandated requirements including NIST, International Standards Organization (ISO), FISMA, the Government Accountability Office (GAO), the Department of Defense (DoD), and Director of Central Intelligence Directive 6/3 Protecting Sensitive Compartmented Information Within Information Systems (DCID 6/3). Security weaknesses can fall into more than one of three categories that include confidentiality, integrity or availability. Security weaknesses and gaps were identified and associated with potential mitigating strategies. Of the 248 requirements evaluated, 144 requirements had an impact on confidentiality, 237 had an impact on Integrity, and 178 had an impact on availability. Of the 248 requirements, 39 were categorized as only having a low impact to security. However, 132 were considered to have a medium impact, and 86 were considered to have a high potential risk.

With 218 findings being of medium to high impact, it is clear that voting data has an unusual security posture. Following the mock election scenario exercise, we derived several conclusions. Voting systems, like many DoD systems, handle sensitive data from all locations worldwide, and therefore, the best protection possible would require that both end points—and the transmission medium—be tightly controlled to maintain data integrity, confidentiality and system availability.

Lastly, without endpoint physical security on the voter side of the equation, any operating systems can be corrupted in time. Despite the presence of antivirus and intrusion prevention technology on most end-user systems, most security holes remain completely unplugged because users do not have sufficient knowledge to secure the operating systems adequately.

Only dedicated, well managed, and often out-sourced, hosting providers blend best of breed technologies capable of identifying potential threats, blended attacks, and distributed denial of service attacks, and are able to escalate quickly to shut down these attacks. However, the communications medium remains a considerable threat to the integrity of the data/votes since it is out of the provider’s control while in transit. At the present, only dedicated communications solutions, with a tightly controlled security posture, such as the Defense Information Systems Network (DISN) would offer such a secure communications channel. Additionally, only dedicated kiosk-based voting stations that are managed and proctored by voting officials can offer a secure endpoint.

FVAP conducted a series of tests over the past year. One test involved the new EAC’s UPPTR dated August 25, 2010. The EAC has the responsibility to develop and implement the certification guidelines to which all voting system manufacturers must adhere. These new EAC UPPTR requirements were developed to serve as a guide to participants in any online pilot voting project. These requirements would provide guidance to pilot project participants regarding what exactly their online pilot project voting system would be required to do. FVAP requested three voting system manufacturers voluntarily subject their system to Voting System Test Lab (VSTL) testing against these new standards. A VSTL is an independent third party accredited as a lab by NIST and certified by the EAC to test voting systems to written standards. The VSTL test was conducted to determine if the requirements were sufficient as written and testable, not to determine if the voting system could pass the new requirements. Section 5.9 of the UPPTR outlines PenTesting and states that systems being tested must be able to pass each portion of section 5.9 in order to pass the VSTL PenTest. The AFIT/RedPhone PenTesting, however, was conducted to determine if the online voting systems could be penetrated to the extent that votes were changed, altered or deleted. The PenTesting section of the UPPTR was used as the testing criteria for passing or failing the PenTest.

In Table 2 below are listed two systems that the VSTLs tested. These two systems were selected by the Director of FVAP to participate in VSTL testing. The AFIT/RedPhone test had three systems. Two of the systems were the systems that the VSTLs tested. One additional vendor was invited to participate in the AFIT/RedPhone test. The table below compares the VSTL testing results and the AFIT/RedPhone PenTesting.

**Table 2. Comparison of VSTL test results and AFIT/RedPhone PenTesting**

5.9 Penetration Resistance	Requirement Matrix	VSTL System 1	VSTL System 2	AFIT System 1	AFIT System 2	AFIT System 3
5.9.1 Resistance to penetration attempts	High, Medium or Low	Medium	Medium	Medium	Medium	Medium
5.9.1.1	The voting system SHALL be resistant to attempts to	Pass	Pass	Pass	Pass	Pass

5.9 Penetration Resistance	Requirement Matrix	VSTL System 1	VSTL System 2	AFIT System 1	AFIT System 2	AFIT System 3
Resistant to attempts	penetrate the system by any remote unauthorized entity.					
5.9.1.2 System information disclosure	The voting system SHALL be configured to minimize ports, responses and information disclosure about the system while still providing appropriate functionality	Pass	Pass	Pass	Pass	Pass
5.9.1.3 System access	The voting system SHALL provide no access, information or services to unauthorized entities.	System Access: All 215 exploits were unsuccessful.	System Access: All 35 exploits were unsuccessful.	Pass	Pass	Pass
5.9.1.4 Interfaces	All interfaces SHALL be penetration resistant including TCP/IP, wireless, and modems from any point in the system.	Interfaces: All 215 exploits were unsuccessful.	Interfaces: All 35 exploits were unsuccessful.	Pass	Pass	Pass
5.9.1.5 Documentation	The configuration and setup to attain penetration resistance SHALL be clearly and completely documented	Documentation: Machine was preconfigured by manufacturer.	Documentation: Machine was preconfigured by manufacturer.	Pass	Pass	Pass
5.9.2 Penetration Resistance Test and Evaluation	High, Medium or Low	Medium	Medium	Medium	Medium	Medium
5.9.1.2 Scope	The scope of penetration testing SHALL include all the voting system components. The scope of penetration testing includes but is not limited to the following:	Scope: Using standard network exploitation tools, all machines and ports were identified.	Scope: Using standard network exploitation tools, all machines and ports were identified.	Pass	Pass	Pass
	System server;	Scope: Using standard network exploitation tools, all machines and ports were identified.	Scope: Using standard network exploitation tools, all machines and ports were identified.	Pass	Pass	Pass
	Vote capture devices;	Scope: Using standard network exploitation tools, all machines and ports were identified.	Scope: Using standard network exploitation tools, all machines and ports were identified.	Pass	Pass	Pass
	Tabulation device;	Scope: Using standard network exploitation tools, all machines and ports were identified.	Scope: Using standard network exploitation tools, all machines and ports were identified.	Pass	Pass	Pass
	All items setup and configured per Technical Data Package (TDP) recommendations;	Scope: Using standard network exploitation tools, all machines and ports were identified.	Scope: Using standard network exploitation tools, all machines and ports were identified.	Pass	Pass	Pass
	Local wired and wireless networks; and	Scope: Using standard network exploitation tools,	Scope: Using standard network exploitation tools,	Pass	Pass	Pass



5.9 Penetration Resistance	Requirement Matrix	VSTL System 1	VSTL System 2	AFIT System 1	AFIT System 2	AFIT System 3
		all machines and ports were identified.	all machines and ports were identified.			
	Internet connections.	Scope: Using standard network exploitation tools, all machines and ports were identified.	Scope: Using standard network exploitation tools, all machines and ports were identified.	Pass	Pass	Pass
5.9.2.2 Test Environment	Penetration testing SHALL be conducted on a voting system set up in a controlled lab environment. Setup and configuration SHALL be conducted in accordance with the TDP, and SHALL replicate the real world environment in which the voting system will be used.	Test Environment: Machines were installed on internal VSTL network.	Test Environment: Machines were installed on internal VSTL network.	Pass	Pass	Pass
5.9.2.3 White Box Testing	The penetration testing team SHALL conduct white box testing using manufacturer supplied documentation and voting system architecture information. Documentation includes the TDP and user documentation. The testing team SHALL have access to any relevant information regarding the voting system configuration. This includes, but is not limited to, network layout and Internet Protocol addresses for system devices and components. The testing team SHALL be provided any source code included in the TDP.	White Box Testing: Vendor documentation was reviewed but no vendor source code was tested.  (The voting system vendors were not asked to supply a source code for review. This section is here because it is a requirement for PenTesting)	White Box Testing: Vendor documentation was reviewed but no vendor source code was tested.  (The voting system vendors were not asked to supply a source code for review. This section is here because it is a requirement for PenTesting)	Not tested by AFIT/RedPhone	Not tested by AFIT/RedPhone	Not tested by AFIT/RedPhone
5.9.2.4 Focus and Priorities	Penetration testing seeks out vulnerabilities in the voting system that might be used to change the outcome of an election, interfere with voter ability to cast ballots, ballot counting, or compromise ballot secrecy. The penetration testing team SHALL prioritize testing efforts based on the following:	Focus and Priorities: Using standard network exploitation tools, all machines and ports were identified. 35 exploits were attempted with no success.	Focus and Priorities: Using standard network exploitation tools, all machines and ports were identified. 35 exploits were attempted with no success.	Pass	Pass	Pass
	a. Threat scenarios for the	Focus and Priorities: Using	Focus and Priorities: Using	Pass	Pass	Pass

5.9 Penetration Resistance	Requirement Matrix	VSTL System 1	VSTL System 2	AFIT System 1	AFIT System 2	AFIT System 3
	voting system under investigation;	standard network exploitation tools, all machines and ports were identified. 35 exploits were attempted with no success.	standard network exploitation tools, all machines and ports were identified. 35 exploits were attempted with no success.			
	b. Remote attacks SHALL be prioritized over in-person attacks;	Focus and Priorities: Using standard network exploitation tools, all machines and ports were identified. 35 exploits were attempted with no success.	Focus and Priorities: Using standard network exploitation tools, all machines and ports were identified. 35 exploits were attempted with no success.	Pass	Pass	Pass
	c. Attacks with a large impact SHALL be prioritized over attacks with a more narrow impact; and	Focus and Priorities: Using standard network exploitation tools, all machines and ports were identified. 35 exploits were attempted with no success.	Focus and Priorities: Using standard network exploitation tools, all machines and ports were identified. 35 exploits were attempted with no success.	Pass	Pass	Pass
	d. Attacks that can change the outcome of an election SHALL be prioritized over attacks that compromise ballot secrecy or cause non-selective denial of service.	Focus and Priorities: Using standard network exploitation tools, all machines and ports were identified. 35 exploits were attempted with no success.	Focus and Priorities: Using standard network exploitation tools, all machines and ports were identified. 35 exploits were attempted with no success.	Pass	Pass	Pass

As Table 2 indicates, the systems tested by the VSTLs maintained an acceptable security posture throughout the PenTesting. The AFIT/RedPhone PenTesting showed similar results. White Box testing was not accomplished by the VSTLs because the voting system vendors were not required as part of their testing to provide a technical data package or submit their source code for review. White Box testing was not accomplished by AFIT/RedPhone for the same reasons.

The results from both the VSTL testing and the AFIT/RedPhone PenTesting suggest the tested voting systems have a good security posture against penetration. No successful penetrations of the systems led to any votes being changed, altered or deleted. This does not mean that manufacturers should be complacent in their security efforts. Each day new cyber threats emerge. A successful electronic voting system must have a very robust security plan and system vendors must continuously strive to improve their security posture throughout the life-cycle of the system.

FVAP continuously works to satisfy its legal mandates and recognizes that some computer science and security experts have strong concerns about security issues associated with online voting. In an effort to move forward and have constructive dialogue on this important topic, FVAP organized the UOCAVA Solutions Working Group (USWG), which brought together a broad cross-section of the election community for constructive discussion on the many associated issues and opportunities for online voting. USWG participants included FVAP, EAC, NIST and other federal agency representatives; voting technology vendors; state and local election officials; computer scientists; political scientists; usability and accessibility specialists; and voting advocates.

FVAP has undertaken three USWG meetings during the past year: August 2010 in Washington, DC prior to the USENIX (Advanced Computing Systems Association) Conference; March 2011 in Chicago prior to the Electronic Verification Network (EVN) workshop; and August 2011 in San Francisco prior to the USENIX Conference. The August 2011 meeting was convened to discuss options for fulfilling 2002 National Defense Authorization Act (NDAA) and the Military and Overseas Voter Empowerment (MOVE) Act of 2009 requirements which authorized FVAP electronic voting pilot programs to test the feasibility of new election technology, and mandated FVAP to carry out an electronic voting demonstration project in which a significant number of uniformed service members could cast ballots in a regularly scheduled election.<sup>i</sup>

The results from both the May 2011 VSTL PenTesting and the August 2011 AFIT/RedPhone PenTesting suggest that the tested online voting systems have the necessary security elements with regard to penetration. There were *no* successful penetrations of any vendor systems that resulted in any vote being changed, altered or deleted. This was a basic computer security expert concern at the USWG meetings and was averted through the AFIT/RedPhone PenTesting exercise.

This does not mean that the tested systems are perfect or that security expert concerns about online voting by are unfounded. However, it does mean the current online voting systems provide a good basis for benchmarking and that more widespread and advanced testing and analysis should be undertaken—in a phased and careful manner—which should include integral and interested members of the election community.

---

<sup>i</sup> For specific information, please go to: <http://www.justice.gov/opa/pr/2010/October/10-crt-1212.html>.

## 5 Recommendations

One of the purposes of the AFIT/RedPhone testing and the VSTL tests mentioned earlier was to determine if the UPPTR requirements are sufficient as written or are in need of revision. Recommended changes to the requirements are shown in Table 4 below. These recommended changes will help voting system manufacturers, the VSTLs, and the EAC to improve online voting system security for systems used in the United States.

**Table 4. Recommended Changes to the UPPTR Security Requirements**

<b>Section 5.9 UPPTR Requirements</b>	<b>Recommended Changes</b>
5.9.1.1 “The voting system SHALL be resistant to attempts to penetrate the system by any remote unauthorized entity”.	Define resistance levels more definitively, utilizing appropriate NIST Special Publication (NIST SP) and by device types and environments within a voting system.
5.9.1.2 “The voting system SHALL be configured to minimize ports, responses and information disclosure about the system while still providing appropriate functionality.”	Define "appropriate functionality" by device types and environments within a voting system. Recommend referencing a NIST SP dealing with hardening.
5.9.1.4 “All interfaces SHALL be penetration resistant including TCP/IP, wireless, and modems from any point in the system.”	Close all ports and shut down all services not needed to perform voting activities.
5.9.2 “Penetration Resistance Test and Evaluation”	This section is oriented toward the VSTL, not the manufacturer. Manufacturers should not be held to the requirement to put in a "Program Manual" that outlines the certification campaign scope.
5.9.2.2 “Penetration testing SHALL be conducted on a voting system set up in a controlled lab environment. Setup and configuration SHALL be conducted in accordance with the TDP, and SHALL replicate the real world environment in which the voting system will be used.”	Requirement is oriented toward the VSTL, not the manufacturer. Manufacturers should not be held to the requirement to put in a "Program Manual" that outlines the certification campaign scope. Some systems are cloud-based, which will be challenging to set up in a controlled lab environment.
5.9.2.3 “The penetration testing team SHALL conduct white box testing using manufacturer supplied documentation and voting system architecture information. Documentation includes the TDP and user documentation. The testing team SHALL have access to any relevant information regarding the voting system configuration. This includes, but is not limited to, network layout and Internet Protocol addresses for system devices and components. The testing team	Requirement is oriented toward the VSTL, not the manufacturer. Manufacturers should not be held to the requirement to put in a "Program Manual" that outlines the certification campaign scope. Some systems are cloud-based, which will be challenging to set up in a controlled lab environment.

SHALL be provided any source code included in the TDP.”	
5.9.2.4 “Penetration testing seeks out vulnerabilities in the voting system that might be used to change the outcome of an election, interfere with voter ability to cast ballots, ballot counting, or compromise ballot secrecy. The penetration testing team SHALL prioritize testing efforts based on the following:	Requirement is oriented toward the VSTL, not the manufacturer. Manufacturers should not be held to the requirement to put in a "Program Manual" that outlines the certification campaign scope. Some systems are cloud-based, which will be challenging to set up in a controlled lab environment.
5.9.2.4.a “Threat scenarios for the voting system under investigation;	Requirement is oriented toward the VSTL, not the manufacturer. Manufacturers should not be held to the requirement to put in a "Program Manual" that outlines the certification campaign scope. Some systems are cloud-based, which will be challenging to set up in a controlled lab environment.
5.9.2.4.b “Remote attacks SHALL be prioritized over in-person attacks;	Requirement is oriented toward the VSTL, not the manufacturer. Manufacturers should not be held to the requirement to put in a "Program Manual" that outlines the certification campaign scope. Some systems are cloud-based, which will be challenging to set up in a controlled lab environment.
5.9.2.4.c “Attacks with a large impact SHALL be prioritized over attacks with a more narrow impact; and	Requirement is oriented toward the VSTL, not the manufacturer. Manufacturers should not be held to the requirement to put in a "Program Manual" that outlines the certification campaign scope. Some systems are cloud-based, which will be challenging to set up in a controlled lab environment.
5.9.2.4. d “Attacks that can change the outcome of an election SHALL be prioritized over attacks that compromise ballot secrecy or cause non-selective denial of service.”	Requirement is oriented toward the VSTL, not the manufacturer. Manufacturers should not be held to the requirement to put in a "Program Manual" that outlines the certification campaign scope. Some systems are cloud-based, which will be challenging to set up in a controlled lab environment.

Most changes above recommend developing a “Program Manual” for VSTL use. This manual would provide guidance to the VSTLs on how the requirements should be set up and tested in a lab environment. The current UPPTR requirements do not tell the manufacturer how to build a system, but rather how the VSTL should organize and prioritize the testing effort. For example, UPPTR requirement 5.9.2.4 has nothing to do with the manufacturer; however, it does tell the VSTL that they SHALL prioritize testing based on certain criteria. The manufacturer should have the required security in place to avoid being penetrated, but the manufacturer should not be held to a standard designed to help the VSTLs conduct a PenTest.

In general, cyber security best practices use mitigation strategies based on a balanced combination of people, operations/processes, and technology. (See page 79 of the U.S. General Accounting Office's (GAO's) *Cybersecurity for Critical Infrastructure Protection* report at <http://www.gao.gov/new.items/d04321.pdf> as just one example of this concept.)

- “People” include the appropriate training, background investigations, clearances, recruitment and retention programs, and incentives.
- “Operations/processes” include written, current, maintained, and management-supported policies and procedures proliferated throughout the organization, as appropriate, so they are vetted and well understood by all involved. Contingency plans and continuity of operations plans also are in this category.
- “Technology” includes software, hardware, telecommunications, anti-malware and alternate paths.

These three dimensions (people, operations/processes, and technology) work together to **prevent** unauthorized confidentiality, integrity, and/or availability degradation; **detect** such degradation when it occurs; and **correct** problems quickly and effectively. At the highest levels, these are basic components of a strong cyber security program. To build such a strong cyber security program, a path forward must be outlined and followed.

The USWG will be presented with the findings of the VSTL testing as well as the AFIT/RedPhone PenTesting. The USWG may recommend some additional testing or perhaps the design of a scientific experiment dealing with the security of online voting systems. The USWG may provide the FVAP Director with some ideas for moving forward with testing online voting security, as well as recommendations on how the industry should work toward the goal of continuous improvement in online voting system security.

The findings, and their importance, should be reviewed and analyzed by cyber security experts experienced in implementing strategies and tactics within government agencies to manage security risk. Such a group of cyber security experts has been formed for this explicit purpose. The Cyber Security Review Group (CSRG) was recruited from DoD, civilian, and intelligence community agencies (e.g., DHS, NSA, DIA, and FBI). This group meets regularly to discuss and analyze cyber security findings related to online voting, and to offer advice on how to reduce risks. This group will add value as an independent government body focused on this project.

FVAP initiated a series of tests that exercised the UPPTR and provided comparative data about the Voting System Test Laboratories (VSTLs). This testing should continue and include the development or validation of software assurance practices used by the voting system manufacturers. It should also include more extensive research into how the EAC developed the UPPTR and how each of the VSTLs interprets sections differently.

FVAP is mandated to produce an electronic voting demonstration project for uniformed UOCAVA voters. This system may potentially be used by UOCAVA voters stationed CONUS (Continental United States) and OCONUS (Outside the Continental United States) voters. It may also be used by forward deployed troops and those afloat. The development life cycle for such a system can take several years to develop, and the initial design and architecture of the system could be complicated. FVAP should

encourage commercial voting system vendors to design and develop a system for the demonstration project. The systems developed should then undergo testing by a VSTL to the UPPTR to ensure the system is compliant with all requirements. Extensive penetration testing that are both lab and operational (within the DOD environment of CONUS, OCONUS, ship board and hostile areas) based should be part of any testing done on the demonstration project system. The participating vendors in this PenTest exercise also fully support future PenTesting efforts by FVAP in an effort to continuously improve their systems.

The demonstration project will define the system; but FVAP must also define the target audience to use the system. FVAP should continue to collect data on the number of UOCAVA voters living abroad with emphasis on uniformed service personnel, as the demonstration project will use uniformed UOCAVA voters as participants. Knowing the number of voters expected to use the system will enable the designers to scale the project according to the participants expected. The designers of the demonstration project will need to know how best to build the system to accommodate the number of voters participating.

## 6 Conclusion

Online voting presents the opportunity for U.S. military service members and their dependents to vote in a timely, effective, and secure manner, regardless of where in the world they may be stationed. However, online voting presents unique security issues because it uses cyber space—computer systems and interconnected networks (such as the internet) to transmit votes.

Before online voting is used, the cyber security risks must be identified and addressed. PenTesting of online voting systems provides an opportunity to proactively identify the threats and address risks.

It is important to state that no penetration attempt was successfully executed. All of the online voting systems that were tested successfully thwarted all attacks posed by the professional RedPhone PenTest team and the trained AFIT students. It is also important to note that this was a modified penetration test, as the time limit was set to 72 hours and no source code review of the vendor's code was conducted. These conditions eliminated any White Box testing from occurring.

This PenTesting exercise did surface both high and low risk issues, as well as some informational concerns. Each issue and concern may need further analysis as circumstances change. Vendors providing online voting systems should apply best security practices to their systems; including full certification and accreditation (C&A) based on government C&A guidance (see NIST and US DoD guidance). Such a C&A requires a formal risk analysis and remediation schedule that is formally tracked by knowledgeable security professionals. Current C&A guidelines require “continuous monitoring” to ensure systems remain at the acceptable security level.

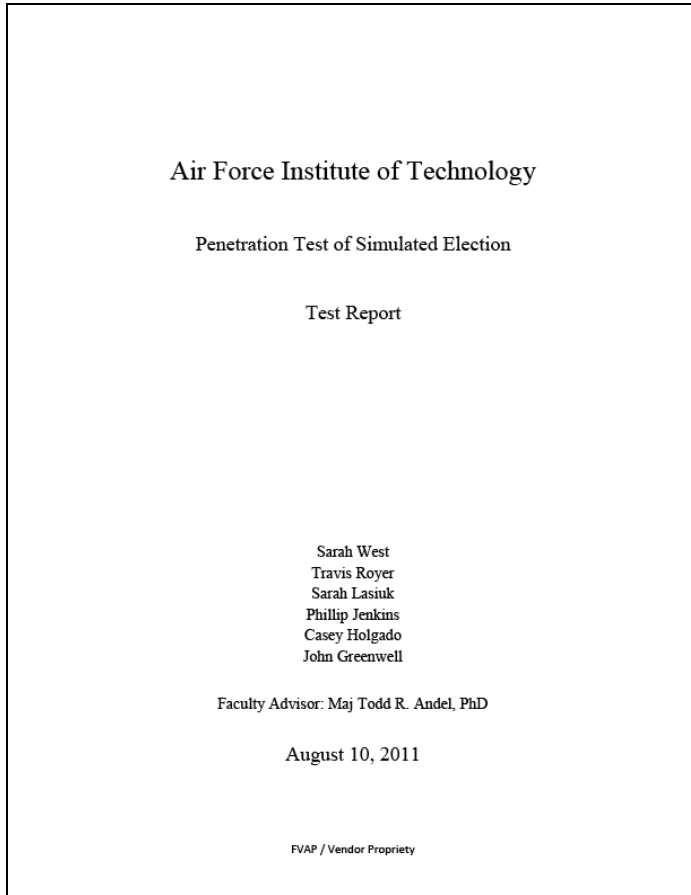
Additionally, PenTests such as the one conducted by AFIT/RedPhone should be undertaken periodically, as online voting systems and attack methods continue to evolve. All of the vendors who participated in this PenTesting exercise fully support this position. Initially, one PenTest should be conducted annually, with increased frequency as time and resources allow, and with an increasing scope. For example, the AFIT/RedPhone PenTest attack lasted only 72 hours (three days). An attack lasting a full week (24/7) should be conducted in the future. Also, a Denial of Service (DoS) attack was not authorized for this particular PenTest. In a real attack scenario, hackers would most certainly launch a DoS attack – if simply to demonstrate that they can succeed in bringing down a system's capability. A DoS attack should be a part of the next PenTest.

Finally, and most importantly, all findings in this, and subsequent PenTests, as well as findings from other types of security analyses, should be addressed, and any risks reduced to acceptable levels by applying the recommendations stated in this report. The AFIT/RedPhone PenTesting exercise was a good first step in demonstrating the security of online voting systems—its strengths and its opportunities for improvement—with qualitative and quantifiable data that will be reviewed at the next USWG meeting, which is yet to be scheduled.



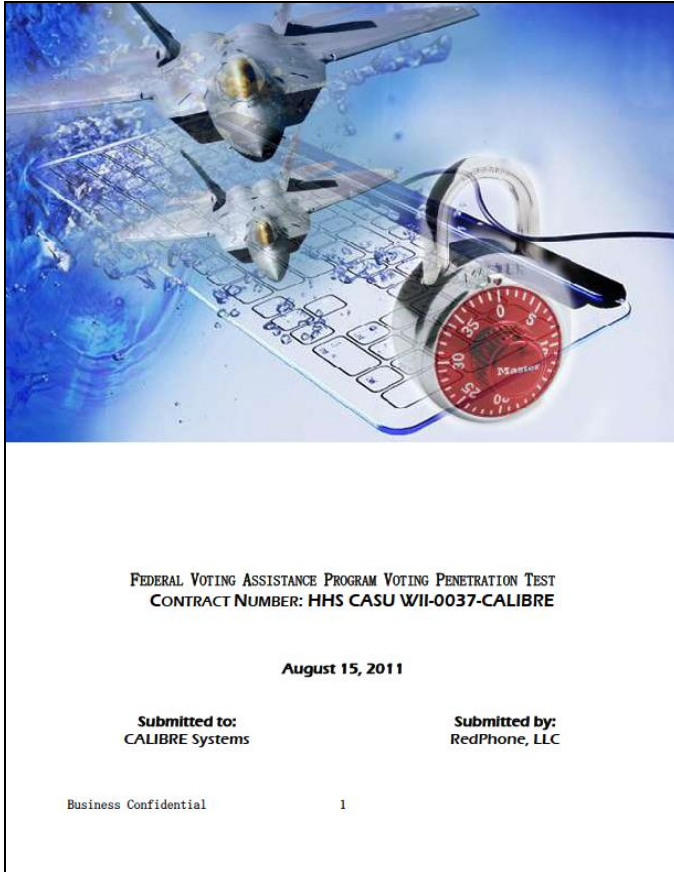
## Appendix A: AFIT Report

To access the AFIT report in PDF format, double-click on the icon below.



## Appendix B: RedPhone Report

To access the RedPhone report in PDF format, double click on the icon below.



## Appendix C: Security Gap Analysis of UOCAVA Pilot Program Testing Requirements

To access the Security Gap Analysis of UOCAVA Pilot Program Testing Requirements report in PDF format, double-click on the icon below.



Adobe Acrobat  
Document