

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 In 2015, Congress eliminated this requirement; however, the resulting reports from the commissioned research remained unpublished at the time of the repeal.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 UPPTTR was studied. Sections two and five of the UPPTTR 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 UPPTTR, 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 Summaryiii

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), 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). 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.

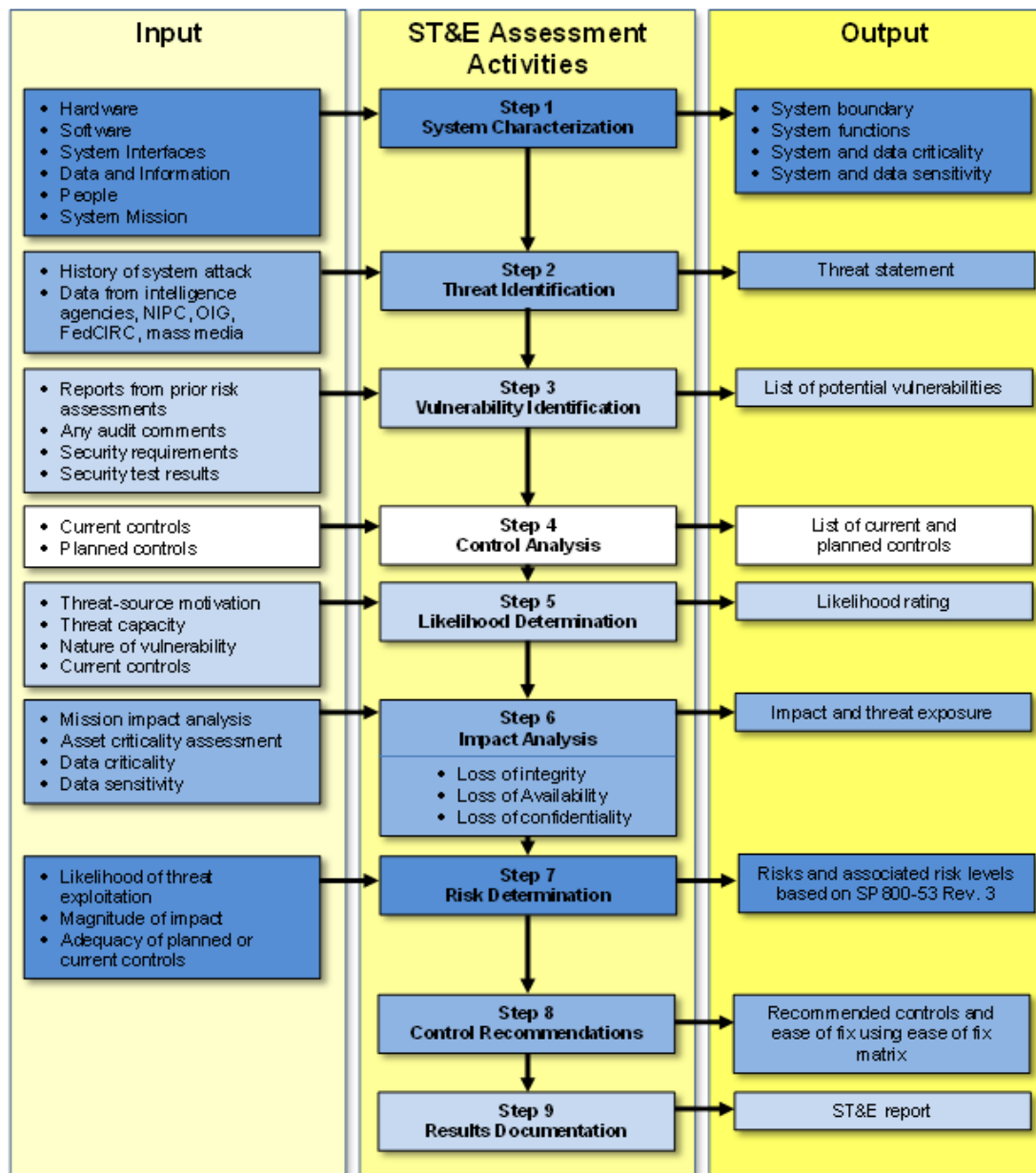


Figure 1. RedPhone Security Test and Evaluation Process

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.

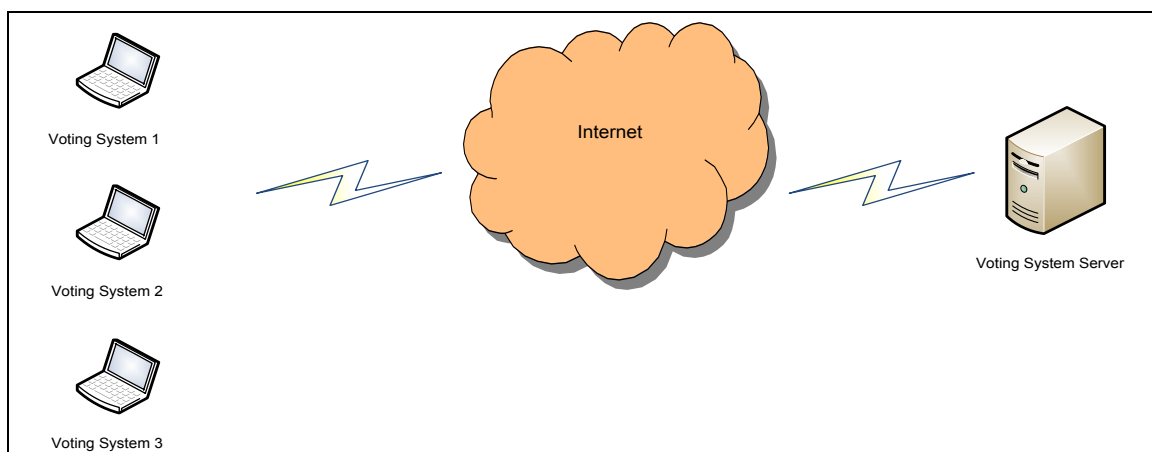
3 Methodology

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.

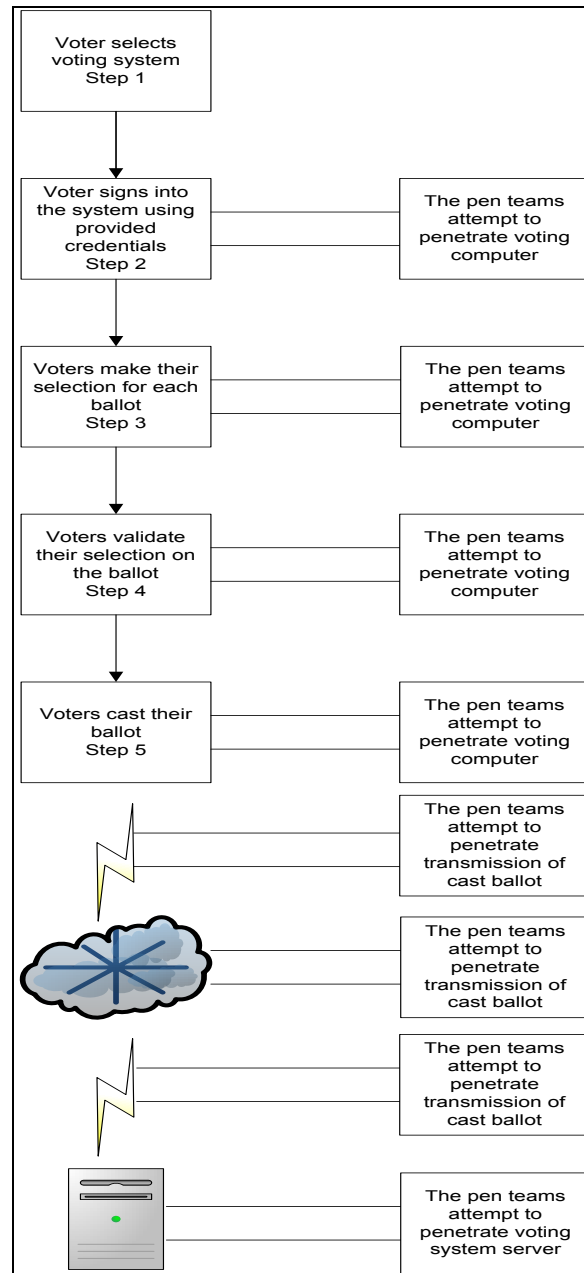


Figure 3. Voter Actions and Penetration Attempts

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 UPPTTR 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 UPPTTR 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 UPPTTR 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 UPPTTR 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.ⁱ

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.

ⁱ 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

Section 5.9 UPPTR Requirements	Recommended Changes
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.

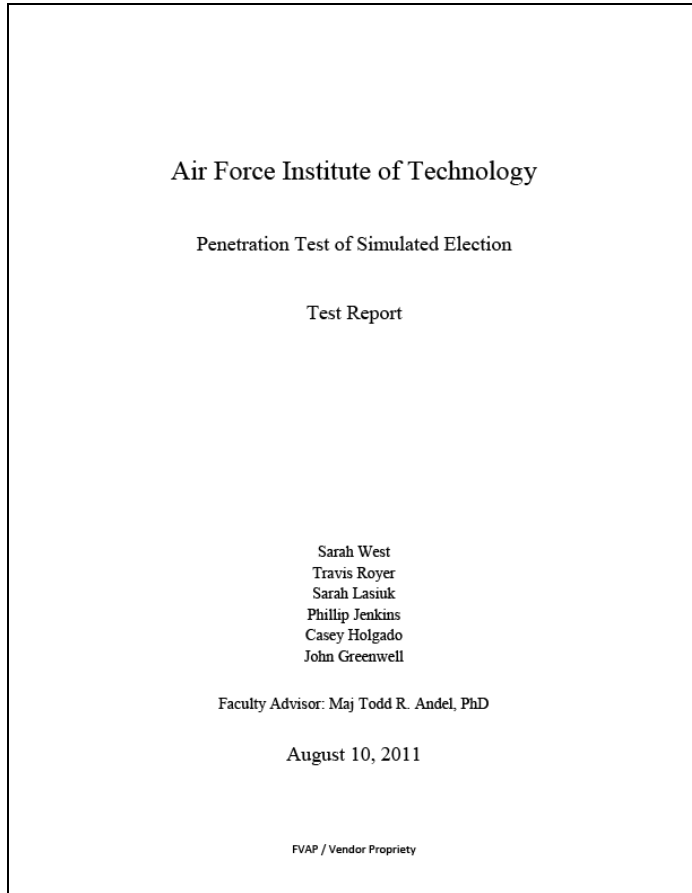
This PenTesting exercise did surface both high and low risk issues, as well as some informational concerns. Each issue and concern may need further analysis as circumstances change. Vendors providing online voting systems should apply best security practices to their systems; including full certification 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.

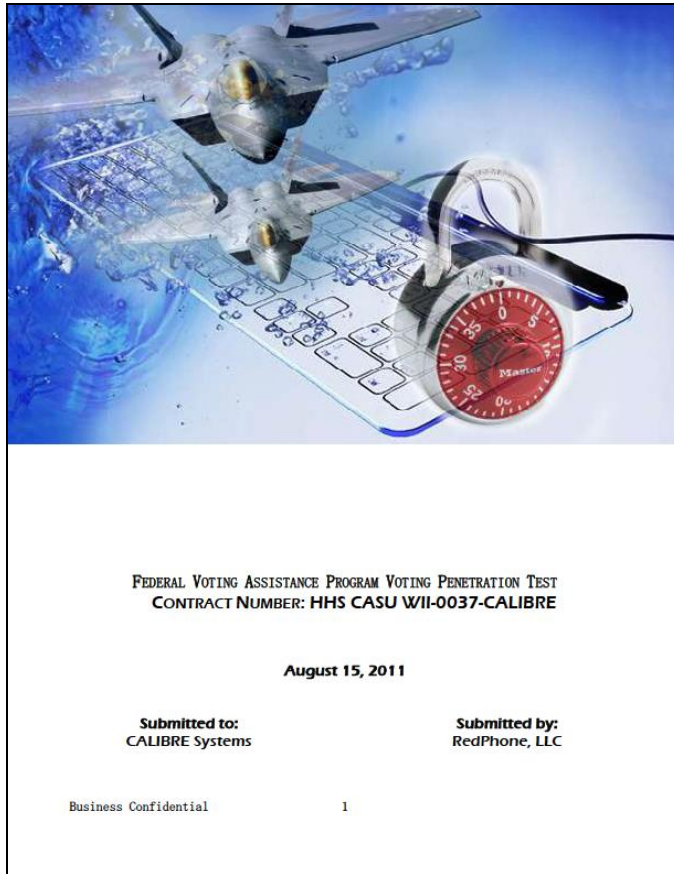
Appendix A: AFIT Report

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

Appendix A

Air Force Institute of Technology

Penetration Test of Simulated Election

Test Report

Sarah West
Travis Royer
Sarah Lasiuk
Phillip Jenkins
Casey Holgado
John Greenwell

Faculty Advisor: Maj Todd R. Andel, PhD

August 10, 2011



Table of Contents

Executive Summary	2
1. Assets of Value	3
2. Vulnerabilities	3
3. Threats	4
4. Impacts/Consequences	6
5. Risk Level	7
6. Recommended Controls	8
7. Conclusion	9
Appendix A	10
Appendix B	21

Executive Summary

This document summarizes the results of a penetration test done by six Air Force ROTC students interning at the Air Force Institute of Technology (AFIT). We conducted this test to help assist the Federal Voting Assistance Program (FVAP). One of FVAP's primary goals is to ensure that overseas active duty uniformed service members and their families may participate in their right to vote overseas through absentee ballots. One of FVAP's goals is to develop a method of voting entirely online, using personal computers. FVAP initiated an effort to test these systems through conducting multiple penetration tests on three different vendors' online voting systems; these vendors are *(to protect the privacy of the vendors, they will be named only as)* Vendor-1, Vendor-2, and Vendor-3. A simulated election was run for a 72 hour-period between August 2-4, 2011. Our goal was to identify and explore any vulnerabilities present within the system and to exploit as many of these vulnerabilities as possible, under certain rules of engagement. With this goal, we attacked the vendors' systems using a variety of methods, logged all of our actions and the results, and prepared them in Appendix A of this report.

The most notable vulnerability was an open Secure Shell (SSH) login prompt on one vendor's servers. Though identified, we were not able to crack it. A host of vulnerabilities were found and tampered with on the laptops simulating the voter machines, including our infiltration with personal administrator accounts. We did not personally succeed in remotely compromising voter confidentiality. We discovered a wide range of information on the servers from NMap and Nessus scans, but none of which were dangerous to security. In the end, we tried many attack vectors, but were not particularly successful. We provided recommendations regarding improvements which can be made to security; but, having not made any prominent breaches in security, we conclude these voting systems to be quite well defended.

1. Assets of Value

The value of penetration testing lies in providing detailed security assessment on real life applications. We tested these voting systems to provide information regarding any potential vulnerabilities that could be present. This test was to establish a risk mitigation framework for any such vulnerabilities identified. In providing our assessments of these risks, we enable the vendors to correct any problems and eliminate vulnerabilities in their software. The process of penetration testing helps to maintain and improve the confidentiality, availability, and integrity of these systems and to determine the effectiveness of their individual security architecture.

2. Vulnerabilities

The most salient vulnerability that we identified was an open Secure Shell (SSH) login that was available on the Vendor-1 voting server. This is a prominent vulnerability because it was an open line to remotely log in to and gain control over the voting server. Anyone on the Internet could potentially connect to this open service.

Physical vulnerabilities abound; any personal voting machine may be tampered with. Each vendor provided a laptop for the simulated voting process. Due to the fact that the voting is not conducted on a well monitored kiosk station, the vendors cannot control the security of the machine on which a voter accesses their voting application via browser. All bets are off when it comes to the voter's machine; both remote threats and physical threats are present. There are no guarantees whatsoever that the voter's machine is free of malware such as rootkits or malicious

viruses. The primary vulnerability that exists in the case of an infected voter machine is that hackers may view the user's input and thereby compromise their confidentiality.

The voting servers hosted by the vendors were unlike the personal voting machines. Some vulnerabilities were identified with scanning software NMap and Nessus. We proved it possible to identify information about the vendor servers. Namely, we were able to scan the servers and identify certificate information, service detection, device type, Hypertext Transfer Protocol information, operating system, and trace route information. These results were not 100% certain, but possessed reasonable reliability. You may refer to Appendix A for each of the vendor's software vulnerabilities found through performing Nessus scans on each of the vendors voting servers.

3. Threats

The open SSH login vulnerability on the Vendor-1 voting server can be easily accessed by anyone connecting to the IP address ([REDACTED]) via PuTTY or other remote login software. A username and password is required, but with enough time an attacker can get around this by brute force. Programs such as Hydra may be used to continually brute force attack the username and password until a successful login is established. Social engineering is also a powerful means of obtaining usernames and passwords relatively easy if employees are untrained in operational security. We did not determine the username or password in our penetration test, and therefore were not able to remotely log in to the Vendor-1 server.

The largest threat that we exploited was the physical security of the machines on which the voters cast their votes. From the first hour of the penetration test we were able to have hands on access to the voting machines with no resistance. We were able to place our own administrator accounts on the machines as well as gather data as the voting systems Internet Protocol (IP) configurations and settings. We were personally able to look over the shoulders of voters and view who they had voted for, thereby compromising the confidentiality of their vote.

Like fore-mentioned as a vulnerability, the fact that the systems allow for remote voting via any Internet-accessible device. Such devices could have various types of malware loaded on it prior to voting, either knowingly or unknowingly, and the possibility of remote keylogging or manipulation of a compromised computer is present. Remote threats open the door to ignorance on the part of the voter. Alone in a windowless room, they may be completely unaware that their vote was observed, or that the attacker cut their connection at the last moment and denied them availability. We were not successful in exploiting any remote threats in any way.

The vulnerability shown by the information we were able to gather is a only an indirect threat. Threats such as this can be valuable to a hacker by informing him what exploits he should utilize. For example, knowing that the server is likely running a Linux kernel narrows the exploits that he will try. Likewise, the knowledge of particular certificates could make a hacker privy to software that may be exploitable. He may also use some of this information in a social engineering attack, i.e. by pretending to be a hardware technician.

4. Impacts/Consequences

An open SSH line would allow a malicious individual command line control over the server. Here, he could explore, change, delete, intercept, download files, upload viruses, and more. He is limited by little more than the rights of the account to which he is logged on (which can be further compromised), his imagination, and his personal skill set once he gains this kind of access. Such exploitation would be a massive compromise of the system's integrity.

If one vote can never be fully secure from being modified, the system does not possess perfect integrity. There are multiple ways integrity of these systems could be potentially compromised. The fact that the voting machine is unsecured could create a devastating impact on the confidentiality of a person's vote for the election. An attacker could load a piece of malware onto a voter's machine that would record how they voted and return the information to the attacker. This could be done remotely on a compromised machine by viewing through a Virtual Network Connection (VNC) window. A second impact using VNC would be that the attacker could take control of the voter's system after the voter logs in. Doing this would allow the attacker to use the voter's session to vote for whoever the attacker wants to win the election.

The impact of the leveraged information collected through scans is proportional to the impact of the exploit. This is wide and varied. By itself, the knowledge that a server is running certain software has little to no impact at all. It all depends on how the information is coupled with exploitation techniques such as hacking attempts and social engineering.

5. Risk Level

We categorize the open SSH server as a *medium* risk. A remote login to the server is a powerful exploitation opportunity for a malicious individual. However, brute forcing a password alone is a task which takes a considerable amount of time, let alone being unaware of both the username and the password. Yet social engineering vectors exist and the SSH command shell is a sumptuous feast for a hacker.

We categorize the threat of remote or physical voting machine exploitation as a *medium* risk. A possible impact of this threat is that an attacker could place malware onto the voter's machine that would compromise the confidentiality of their vote. The risk level for this is noteworthy, considering the fact that many users do not update their computers or keep them completely secure. The voting application uses a Hypertext Transfer Protocol Secure (HTTPS) connection that offers protection from the vote data being sniffed, however an attacker can simply view the vote from a VNC shell on the local host as it is taking place. A second consequence was also noted, stating that an attacker could take control the voter's session once they log in, allowing the attacker to vote for who they want to win or denying the right for the voter to cast their legal vote. Even though this would be an easy task for an attacker to do, they may opt not to use it due to the fact that it would be visibly obvious when it happens and the election results would probably be voided. Compromising an insecure system is a fairly easy task, and there is no way of enforcing the user to make sure that their computer is secure prior to voting. Although we were not able to successfully compromise the vendor's systems, these possibilities are always a threat. No vote over such open networks can have complete confidentiality, but public eyes expect 100% and view any loss as calamitous.

We categorize information gained through scanning as a *low* risk. This information is by no means privileged and carries little weight on its own. The knowledge it provides is small in comparison to the working knowledge required for high-risk exploitations.

6. Recommended Controls

We recommend the immediate removal of the SSH login available on the Vendor-1 voting server. If it is necessary that it remain open, the password and username should be frequently changed. Furthermore, the rights provided in the command shell should be as low as possible required to meet its purpose.

Complete security on the voter's machine is not possible. However, as the voter is beginning the process, prior to entering their confidential information, they should be instructed on steps that they may take to ensure immunity to common threats. We recommend the delivery of flags and warnings should the voting client detect that the user lacks antivirus or antispyware programs.

Voters' worries can be further calmed by accessibility to the vendor's help and technical support lines where they can be directed to methods of removing malware. It may also be wise to limit the amount of time a voter may be logged in to the voter application to reduce the chance of exploitation.

If possible, it would be wise to limit the information accessible by NMap and Nessus scans. The less a hacker can determine through scans, the less vulnerable the voting servers are. In fact, the vendors may use deception; by this, they may not only dissuade attackers, but divert them into dead ends. Thus, informational scans can be used as a reverse means against potential attackers.










7. Conclusion

In conclusion, we found the vendors Vendor-1, Vendor-2, and Vendor-3 to be admirably secure. Though vulnerabilities were identified in our test, we were unsuccessful in our attempts to exploit and did not achieve compromised systems. Within this report we specified the value of the three voting system vendors on both their confidentiality as well as integrity of each system. We identified low and medium level securities including an open SSH line and information about the machines running the systems. We discovered these threats by conducting reconnaissance and gaining physical access to the three vendor's end kiosk clients, and we elaborated on their impact in this document. Lastly, we suggested recommended controls on these systems such as limiting the amount of time on the servers and possibly the amount of information available on scanning tools open to the public such as Nessus and NMap. The logs of our attacks and scans are shown below in Appendix A and B, respectively.

Appendix A

Penetration Test Time Log

Vendor-3 Time Log			
Date: 8/2/2011			
Time	Action	Outcome	Team Member
815	Placed vote on voting workstation	Gather details on how voting process works	A
820	Placed vote on voting workstation	Gather details on how voting process works	C
820	Explored target workstations and retrieved the IP addresses of the targeted internal voting workstation	Internal IP Address [REDACTED]	D
820	Attempted to establish a new user account on the target workstation	Unsuccessful at creating a new user	D
830	Used command <i>ipconfig</i> in command prompt of voting workstation to obtain IP address of target computer	Internal IP Address [REDACTED]	A
830	Created account on voting workstation with administrative access	User Name: Support ; Password: H01GaD0	B
830	Placed vote on voting workstation	Gather details on how voting process works	B
830	Logged internal IP address of voting workstations	Internal IP Address: [REDACTED]	B
845	Scanned the internal voting workstation at [REDACTED] using Nessus		D
848	Scanned the external vendor web server at [REDACTED] using Nessus	See Appendix B for report of vulnerabilities	D
852	Ran internal scan on [REDACTED] using Nessus		A
900	Retrieved voting system web address	https:// [REDACTED]	A
900	Used command <i>ping</i> [REDACTED] in command prompt to verify communication with target internal voting workstation	Successful response and verification of communication established	B
913	Scanned the internal voting workstation at [REDACTED] using Nmap		E
919	Downloaded PsTools for Windows and ran the command <i>psexec \\ [REDACTED] Support cmd</i> in command prompt of each internal IP address	Connection failed and was unable to connect to desired destination	A
920	Started Cain	Found a workgroup called VENDOR-3_INT with one XP computer named COMP023	C

930	Used command prompt to ping URL 	Discovered the IP address of voting system server which is 	B
935	Ran the command <i>mstsc</i> in command prompt	Unable to connect to and establish a remote desktop on 	A
958	Ran a PHP meterpreter, Reverse TCP Incline exploit in Metasploit on internal voting workstation	Unable to exploit target	D
1000	Ran external scan on  using Nessus		A
1000	Attempted to establish connection to internal voting workstation using the command <i>windows/smb/psexec/reverse_tcp</i> in Metasploit	Failed to establish a connection	B
1000	Ran a PHP meterpreter, Reverse TCP Sager exploit in Metasploit on internal voting workstation	Unable to exploit target	D
1010	Ran a multi/handler SSL exploit with payload of meterpreter_reverse_TCP in Metasploit on internal voting workstation	Unable to exploit target	D
1030	Ran internal scan on  using Nessus	Low vulnerabilities reported	B
1030	Ran a <i>vlc_smb_url</i> msf exploit with payload of meterpreter_reverse_TCP in Metasploit on internal voting workstation	Unable to exploit target	D
1045	started intense, all tcp on Vendor-3 laptop	was interrupted	F
1100	Ran scan on internal IP address  using Nmap		A
1100	Scanned the voting system URL using Sitedigger	No Vulnerabilities found	B
1125	Ran a slow internal scan on the internal workstation IP  using Nmap	See Appendix B for results	E
1130	Scanned  using an intense scan with Nmap		B
1300	Ran an external scan on the voting system website server using Nessus	No Vulnerabilities found	B
1302	tried to visit Vendor-3.com	failed-timed out	F
1305	Used Maltego and began running all transforms on Vendor-3.com	results gathered; no salient breakthroughs	F
1316	started nmap -T4 -A -v -PN  Vendor-3.com	started	F
1320	nMap completed	results saved, some interesting data, few conclusive, no breakthroughs	F
1330	Ran a SQL injection scan on voting system website using Webcruiser		B

1330	Used Blackwidow and Foca tools in order to crawl the vendor website and look for additional vulnerabilities		C
1400	Completed SQL injection scan on voting system website using Webcruiser	No Vulnerabilities found	B
1406	Attempted to scan range of IP addresses for network which the voting system web server is located [REDACTED] using Nmap	Scan never completed	E
1430	Ran scan on web server [REDACTED] using Nmap		B
1449	Scanned the external IP [REDACTED] using Nessus	No Vulnerabilities found	E
1500	Completed scan on web server [REDACTED] using Nmap	Discovered that the Vendor-3 system is running Windows	B
1505	Scanned the external IP [REDACTED] using Nessus	See Appendix A for results	E

Date: 8/3/2011			
Time	Action	Outcome	Team Member
900	Manually changed settings on voting workstation to allow remote desktop connection and added the user "Support" to list of users that may access it		A
951	Attempted to ping internal workstation IP [REDACTED] using the command prompt	No response to ping	E
935	sent fake email to Vendor-3@Vendor-3.com as jason mulbrich, attempted to gain insight into workforce for social engineering	sent; no reply ever received	F
950	sent fake email to [REDACTED]@Vendor-3.com as "MS Outlook"	failed	F
958	Attempted to ping internal workstation IP [REDACTED] using the command prompt	No response to ping	E
1000	Attempted to remote desktop into voting workstation	Unsuccessful connection	A
1000	Attempted to ping the internal voting workstation IP [REDACTED] using the command prompt	No response from the target IP address	A
1000	Ran intense scan on the internal voting workstation IP [REDACTED] using Nmap		B
1013	Attempted to ping the internal voting workstation IP [REDACTED] using the command prompt	Response back from targeted IP	E
1030	Ran scan on the internal voting workstation IP [REDACTED] using Nessus		B
1300	Ran scan on the internal voting workstation IP [REDACTED] using Armitage		B

1322	sqlite3 db_nmap scan of Vendor-3 laptop in BT4	completed in 40s, results gathered as before	F
1323	db_autopwn -p -t -e of Vendor-3 laptop	completed in 6seconds no sessions	F
1400	Ran Hail Mary exploit on the internal voting workstation IP [REDACTED] using Armitage		B
1500	Scanned the external IP [REDACTED] using Nmap		B

Date: 8/4/2011

Time	Action	Outcome	Team Member
816	Scanned the internal voting workstation IP [REDACTED] using Nmap -p 1-65535 command on Nmap		B
826	Scanned the internal voting workstation IP [REDACTED] using Nmap -5T -A -v command on Nmap		B
1000	started nmap scan of Vendor-3 server, intense scan no ping except -T4 changed to -T2 for stealth	started	F
1002	prematurely stopped nessus scan of Vendor-3 server (started about 30 mins prior)	results gathered, 14 vulnerabilities 1 med 13 low	F
1030	nmap scan of Vendor-3 server done	results lost... zenmap crashed	F
1052	nmap scan of Vendor-3 server again, intense scan no ping -T2	started	F
1054	nmap scan of Vendor-3 server done	results saved	F

Vendor-1 Time Log			
Date: 8/2/2011			
Time	Action	Outcome	Team Member
815	Placed vote on voting workstation	Gather details on how voting process works	A
820	Placed vote on voting workstation	Gather details on how voting process works	C
820	Retrieved voting system web address	https:// [REDACTED]	C
820	Pinged URL to retrieve external IP address	Discovered the IP address of voting system server which is [REDACTED]	C
820	Explored target workstations and retrieved the IP addresses of the targeted internal voting workstation	Internal IP Address: [REDACTED]	D
820	Vendor-1 laptop voting server: attempt SQLI 'or'1='1'*/ 'or'1='1'{' 'or'1='1'/'	invalid	F
820	Attempted to establish a new user account on the target workstation	Unsuccessful at creating a new user	D
830	Used command <i>ipconfig</i> in command prompt of voting workstation to obtain IP address of target computer	Internal IP Address: [REDACTED]	A
830	Created account on voting workstation with administrative access	User Name: Support ; Password: H01GaD0	B
830	Placed vote on voting workstation	Gather details on how voting process works	B
830	Logged internal IP address of voting workstations	Internal IP Address: [REDACTED]	B
850	Ran internal scan on [REDACTED] using Nessus		A
851	Pinged URL to retrieve external IP address	Discovered the IP address of voting system server which is [REDACTED]	D
855	Scanned the external vendor web server at [REDACTED] using Nessus	No Vulnerabilities found	D
900	Retrieved voting system web address	https:// [REDACTED]	A
900	Gathered URL for voting site	https:// [REDACTED]	B
900	Used command <i>ping</i> [REDACTED] in command prompt to verify communication with target internal voting workstation	Successful response and verification of communication established	B
900	Used command prompt to ping the URL https:// [REDACTED]	Discovered the IP address of voting system server which is [REDACTED]	B
900	Used PuTTY to connect to port 22 (SSH) on vendor web server	Received a prompt for login	D
919	Downloaded PsTools for Windows and ran the command <i>psexec</i> \\ [REDACTED] -u Support cmd in command prompt of each internal IP address	Connection failed and was unable to connect to desired destination	A

920	Went to http://testbed.Vendor-1.com/robots.txt in web browser	Browser displayed- user-agent: * Disallow: /	E
935	Ran the command <i>mstsc</i> command prompt	Unable to connect to and establish a remote desktop on [REDACTED]	A
957	Ran a slow internal scan on the internal workstation IP [REDACTED] using Nmap	See Appendix B for results	E
958	Ran a web app scan on voting site using Nessus	No Vulnerabilities found	E
1000	Ran external scan on [REDACTED] using Nessus		A
1000	Attempted to establish connection to internal voting workstation using the command <i>windows/smb/psexec/reverse_tcp</i> in Metasploit	Failed to establish a connection	B
1000	Used autopwn consisting of over 100 exploits on the web server [REDACTED] in order to establish a connection	No successful connection made	C
1005	nessus scan against server complete	2 low vulnerabilities	F
1005	Lost connection with voting site		E
1030	Ran internal scan on [REDACTED] using Nessus	Low vulnerabilities reported	B
1040	Scanned the external web server IP [REDACTED] using Nmap	See Appendix B for results	D
1050	Scanned the external web server IP [REDACTED] using Nessus	See Appendix B for results	D
1100	Ran scan on internal IP address [REDACTED] using Nmap		A
1100	Scanned the voting system URL using Sitedigger	No Vulnerabilities found	B
1130	Scanned [REDACTED] using an intense scan with Nmap		B
1134	Scanned the internal voting workstation at IP [REDACTED] using Nessus		D
1300	Ran an external scan on the voting system website server using Nessus	No Vulnerabilities found	B
1330	Ran a SQL injection scan on voting system website using Webcruiser		B
1330	Used Blackwidow and Foca tools in order to crawl the vendor website and look for additional vulnerabilities		C
1400	Completed SQL injection scan on voting system website using Webcruiser	No Vulnerabilities found	B

1420	Discovered administrative login page for Vendor-1.com	The administrative directory was listed in robots.txt for the website; Login page was a website built with Joomla software; Noted webpage source code uses Joomla 1.5	C
1430	Ran scan on web server [REDACTED] using Nmap		B
1500	Completed scan on web server [REDACTED] using Nmap	Discovered that the Vendor-1 voting system is running Linux	B
1500	Attempted the Joomla 1.5 password reset token vulnerability on administrative login page	Failed attempt- website was patched to prevent this	C
1530	attempted metasploit psexec on EC laptop	no reply	F
1540	Ran a Joomla automated attack tool on the administrative login page	No Vulnerabilities found	C

Date: 8/3/2011			
Time	Action	Outcome	Team Member
850	Attempted to ping internal workstation IP [REDACTED] using the command prompt	No response to ping; Problem with laptop	E
900	Used Vendor-1.com/index.php?option=com_NAME to see if webpage returned a 404 error or blank page	only component found: com_jce	C
900	Found a vulnerability for the com_jce component via Exploit-DB	SQL injection failed- the vulnerability was patched; continued running Hydra remote brute force	C
908	Scanned the internal voting workstation IP [REDACTED] using stealthy scan in Nmap		D
1000	Ran intense scan on the internal voting workstation IP [REDACTED] using Nmap		B
1030	Ran scan on the internal voting workstation IP [REDACTED] using Nessus		B
1300	Ran scan on the internal voting workstation IP [REDACTED] using Armitage		B
1400	Ran Hail Mary exploit on the internal voting workstation IP [REDACTED] using Armitage		B
1440	Remote SSH puTTY attempt into Vendor-1 server [REDACTED]	opened login screen, attempted root and five passwords; failure	F
1500	Scanned the external IP range [REDACTED] using Nmap		B

Date: 8/4/2011			
Time	Action	Outcome	Team Member
820	Scanned the internal voting workstation IP : [REDACTED] using Nmap -p 1- 65535 command on Nmap		B

Vendor-2 Time Log			
Date: 8/2/2011			
Time	Action	Outcome	
815	Placed vote on voting workstation	Gather details on how voting process works	A
820	Placed vote on voting workstation	Gather details on how voting process works	C
820	Retrieved voting system web address	https:// [REDACTED]	C
820	Pinged URL to retrieve external IP address	Discovered the IP address of voting system server which is [REDACTED]	C
820	Explored target workstations and retrieved the IP addresses of the targeted internal voting workstation	Internal IP Address: [REDACTED]	D
820	Attempted to establish a new user account on the target workstation	Unsuccessful at creating a new user	D
830	Used command <i>ipconfig</i> in command prompt of voting workstation to obtain IP address of target computer	Internal IP Address: [REDACTED]	A
830	Created account on voting workstation with administrative access	User Name: Support ; Password: H01GaD0	B
830	Placed vote on voting workstation	Gather details on how voting process works	B
830	Logged internal IP address of voting workstations	Internal IP Address: [REDACTED]	B
850	Ran external scan on [REDACTED] using Nessus	Had open ports: 22, 80, 443	C
850	Used PuTTY to try and connect to Port 22 (SSH) on [REDACTED]	Received Login Prompt	C
853	Ran internal scan on [REDACTED] using Nessus		A
900	Retrieved voting system web address	https:// [REDACTED]	A
900	Used command <i>ping</i> [REDACTED] in command prompt to verify communication with target internal voting workstation	Successful response and verification of communication established	B
915	nessus scan run against Vendor-2 laptop, saved results	3 low vulnerabilities	0
900	Made basic login attempts within the login prompt received when connecting to Port 22 (SSH) on [REDACTED] with PuTTY: User Names- Admin, Administrator, root, user ; Passwords- blank, same input as username	No successful match	C
919	Downloaded PsTools for Windows and ran the command <i>psexec \\ [REDACTED] -u Support cmd</i> in command prompt of each internal IP address	Connection failed and was unable to connect to desired destination	A

930	Used Command prompt to ping URL https:// [REDACTED]	Discovered the IP address of voting system server which is [REDACTED]	B
935	Ran the command <i>mstsc</i> in command prompt	Unable to connect to and establish a remote desktop on [REDACTED]	A
940	Went to http:// [REDACTED] in web browser	Discovered later that we wanted [REDACTED] instead of [REDACTED]	E
950	Began running Hydra to attempt to brute-force the Login dialog prompted when connecting to Port 22 (SSH) with PuTTY: Defined Usernames- Administrator, user, root ; Passwords- 1.7 million common passwords file	No successful match	C
1000	Ran external scan on [REDACTED] using Nessus		A
1000	Attempted to establish connection to internal voting workstation using the command <i>windows/smb/psexec/reverse_tcp</i> in Metasploit	Failed to establish a connection	B
1030	Ran internal scan on [REDACTED] using Nessus	Low vulnerabilities reported	B
1038	attempted BT5 psexec exploit on Vendor-2 laptop	failed-timed out	F
1044	Ran a slow internal scan on the internal workstation IP [REDACTED] using Nmap	See Appendix B for results	E
1053	Scanned the external web server IP [REDACTED] using Nessus	See Appendix B for results	D
1055	Scanned the external web server IP [REDACTED] using Nmap	See Appendix B for results	D
1100	Ran scan on internal IP address [REDACTED] using Nmap		A
1100	Scanned the voting system URL using Sitedigger	No Vulnerabilities found	B
1126	Ran exploit Windows/smb/ms09_050smb2 on internal voting workstation using Metasploit	Unable to exploit vulnerability	D
1130	Scanned [REDACTED] using an intense scan with Nmap		B
1135	Scanned the internal voting workstation at IP [REDACTED] using Nessus		D
1240	Pinged URL using command prompt to verify response from voting website	Successful response and verification of communication established	D
1300	Ran an external scan on the voting system website server using Nessus	No Vulnerabilities found	B
1312	Attempted to scan range of IP addresses for network which the voting system web server is located [REDACTED] using Nmap	Scan never completed	E

1330	Ran a SQL injection scan on voting system website using Webcruiser		B
1330	Used Blackwidow and Foca tools in order to crawl the vendor website and look for additional vulnerabilities		C
1400	Completed SQL injection scan on voting system website using Webcruiser	No Vulnerabilities found	B
1430	Ran scan on web server [REDACTED] using Nmap		B
1500	Completed scan on web server [REDACTED] using Nmap	Discovered that the Vendor-2 system is running Linux	B
1540	Scanned the external IP [REDACTED] using Nessus	See Appendix B for results	E
1544	Scanned the external IP [REDACTED] using Nessus	No Vulnerabilities found	E

Date: 8/3/2011			
Time	Action	Outcome	Team Member
1000	Ran intense scan on the internal voting workstation IP [REDACTED] using Nmap		B
845	Attempted to ping internal workstation IP [REDACTED] using the command prompt	No response to ping; Problem with laptop	E
958	Scanned the internal voting workstation IP [REDACTED] using Nmap		D
1030	Ran scan on the internal voting workstation IP [REDACTED] using Nessus		B
1300	Ran scan on the internal voting workstation IP [REDACTED] using Armitage		B
1400	Ran Hail Mary exploit on the internal voting workstation IP [REDACTED] using Armitage		B
1500	Scanned the external IP range [REDACTED] using intense scan in Nmap	No response to ping	B

Date: 8/4/2011			
Time	Action	Outcome	Team Member
820	Scanned the internal voting workstation IP [REDACTED] using Nmap -p 1-65535 command on Nmap		B

Appendix B

NMap Scans of Vendor Systems

Vendor-2 Internal Computer Nmap Scan

Nmap Scan Report- Scanned at Wed Aug 03 10:06:38 2011

Scan Summary

Scan Summary

Nmap 5.51 was initiated at Wed Aug 03 10:06:38 2011 with these arguments:
nmap -T4 -A -v -PE -PS?2,25,80 -PA21,2;3,BQ, [REDACTED]

Verbosity: 1; Debug level 0

Address

Ports

The 1000 ports scanned but not shown below are in state: **filtered**

Remote Operating System Detection

Used port: 43127 /udp (closed)
OS match: Microsoft Windows Server 2006 (66%)
OS match: Microsoft Windows Server 2006 R2 (66%)
OS match: Microsoft Windows Server 2006 SP1 (66%)
OS match: Microsoft Windows Server 2006 SP2 (66%)
OS match: Microsoft Windows 7 (66%)
OS match: Microsoft Windows 7 Professional (88%)
OS match: Microsoft Windows 7 Ultimate (88%)
OS match: Microsoft Windows Longhorn (66%)
OS match: Microsoft Windows Vista (66%)
OS match: Microsoft Windows Vista Business (88%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

Vendor-2 ServerNmap Scan

Nmap Scan Report- Scanned at Wed Aug 03 14:25:49 2011

Scan Summary 1 [REDACTED]

Scan Summary

Nmap 5.51 was initiated at Wed Aug 03 14:25:49 2011 with these arguments:
`nmap -T5 -A -v -Pn [REDACTED]`

Verbosity: 1; Debug level 0

[REDACTED]

Address

[REDACTED] (ipv4)

Ports

The 1000 ports scanned but not shown below are in state: filtered

Remote Operating System Detection

Unable to identify operating system.

Traceroute Information (click to expand)

Misc Metrics (click to expand)

[REDACTED]

Vendor-1 Internal Computer Nmap Scan

Nmap Scan Report - Scanned at Wed Aug 03 09:56:36 2011

Scan Summary

Scan Summary

Nmap 5.51 was initiated at Wed Aug 03 09:56:36 2011 with these arguments:
`nmap -T4 -A -v -PE -PS22, [REDACTED]`

Verbosity: 1; Debug level 0

Address

[REDACTED] (ipv4)

Ports

The 1000 ports scanned but not shown below are in state: **filtered**

Remote Operating System Detection

Used port: **42942/udp (closed)**
OS match: **Microsoft Windows Server 2008 (89%)**
OS match: **Microsoft Windows Server 2008 R2 (89%)**
OS match: **Microsoft Windows Server 2008 SP1 (89%)**
OS match: **Microsoft Windows Server 2008 SP2 (89%)**
OS match: **Microsoft Windows 7 (89%)**
OS match: **Microsoft Windows 7 Professional (89%)**
OS match: **Microsoft Windows 7 Ultimate (89%)**
OS match: **Microsoft Windows Longhorn (89%)**
OS match: **Microsoft Windows Vista (89%)**
OS match: **Microsoft Windows Vista Business (89%)**

Traceroute Information (click to expand)

Misc Metrics (click to expand)

Vendor-1 ServerNmap Scan

Nmap Scan Report- Scanned at Thu Aug 04 09:25:06 2011

Scan Summary | lwdc.dbo2.fa1 34.host4. 24396 [REDACTED]

Scan Summary

Nmap SSI was initiated at Thu Aug 04 09:25:06 2011 with the-se arguments:

P"l<<l> :.i. :A.v *Pn ZJQ.JJ/\$.4lj

Verbosity:1: Debug level 0

[REDACTED] / lwdc.dbo2.fa1-34.host4. 24396 [REDACTED]

Address

[REDACTED] * (ipv4)

Hostnames

lwdc.dbo2.fa1-34.host4.24396 [REDACTED] (PTR)

Ports

The 999 ports scanned but not shown below are in state: **filtered**

State (toggle closed (0) I filtered (0))

o n

Product

Aj>ache httpd

Remote Operating System Detection

use<l port: 443/tcp (open)
OS match: Unix x.x.x- x.x.xx (94%)
OS match: Unix x.x.x- x.x.xx (92%)
OS match: Unix x.x.x- x.x.xx (89%)
OS match: Linux x.x.xx (CentOS 5, x86_64, SHP) (89%)
OS match: ZoneAlarm Z100G WAP (89%)
OS match: linux x.x.xx (CentOS 5.2) (88%)
OS match: Unwc x.x.x- xxx.stabxxx.xx-enterpri.se (CentOS 4.2 x:86) (86%)
OS match: Unix x.x.x- x.x.xx (88%)
OS match: Unix x.x.xx (Centos 5.3) (88%)

Traceroute Information (click to expand)

Host Metrics (click to expand)

Vendor-3 Internal Computer Nmap Scan

Nmap Scan Report- Scanned at Wed Aug 03 10:12:33 2011

Scan Summary

Scan Summary

Nmap 5.51 was initiated at Wed Aug 03 10:12:33 2011 with these arguments:
omaR -T4 -A -v -PE -PSZ2 - 80 -PA21.2J,S0,338

Verbosity: 1; Debug level 0

Address

Ports

The 1000 ports scanned but not shown below are in state: **filtered**

Remote Operating System Detection

Used port: 40114/udp (closed)
OS match: Microsoft Windows Server 2008 (89%)
OS match: Microsoft Windows Server 2008 R2 (89%)
OS match: Microsoft Windows Server 2008 SP2 (89%)
OS match: Microsoft Windows Server 2008 SP2 (89%)
OS match: Microsoft Windows 7 (89%)
OS match: Microsoft Windows 7 Professional (89%)
OS match: Microsoft Windows 7 Ultimate (89%)
OS match: Microsoft Windows Longhorn (89%)
OS match: Microsoft Windows Vista (89%)
OS match: Microsoft Windows Vista Business (89%)

Traceroute Information (click to expand)

Misc Metrics (click to expand)

Vendor-3 ServerNmap Scan

Nmap Scan Report- Scanned at Wed Aug 03 14:28:30 2011

Scan Summary 1 [REDACTED]

Scan Summary

Nmap 5.51 was initiated at Wed Aug 03 14:28:30 2011 with these arguments:
`nmap -T5 -A -v -Pn [REDACTED]`

Verbosity: 1; Debug level: 0

[REDACTED]

Address

[REDACTED] (ipv4)

Ports

The 999 ports scanned but not shown below are in state: filtered

State (toggle closed (O) | filtered (F))
open

Remote Operating System Detection

Used port: 443/tcp (open)
OS match: HP 170X print server or Inkjet 3000 printer (94%)
OS match: Crestron XPanel control system (90%)
OS match: Netgear OG834G WAP (90%)
OS match: Nintendo Wii game console (86%)
OS match: Vodavi XTS-IP PBX (86%)
OS match: Brother MFC-7620N multifunction printer (65%)
OS match: Microsoft Xbox game console (modified, running XboxMediaCenter) (55%)
OS match: Hirschmann L2E Railswitch (85%)

Traceroute information (click to expand)
Misc Metrics (click to expand)



Nessus Scans of Vendor Servers

1. Vendor-2 System Server:



1.1 Port 0- TCP

1.2. Port 0- UDP



2. Vendor-1 Server:



2.1. Port 0- TCP

2.2. Port 0- UDP



2.3 Port 80- TCP

2.4. Port 443- TCP

3. Vendor-3 Server:



3.1. Port 0 – TCP

3.2. Port 0- UDP



3.3. Port 21-TCP

3.4. Port 25- TCP

3.5. Port 53- TCP

3.6. Port 443- TCP

3.7. Port 993- TCP

3.8.Port 5432- TCP

The screenshot shows the Nessus web interface. The 'Reports' tab is active. On the left, under 'Ports / Protocols', the entry '5432 / tcp' is selected. The main area displays a table with one result:

Plugin ID	Name	Port	Severity
26024	PostgreSQL Server Detection	postgres (5432)	Low

At the top right of the results area, it says '1 results'.

Appendix B



FEDERAL VOTING ASSISTANCE PROGRAM VOTING PENETRATION TEST
CONTRACT NUMBER: HHS CASU WII-0037-CALIBRE

August 15, 2011

Submitted to:
CALIBRE Systems

Submitted by:
RedPhone, LLC

POINT OF CONTACT: L. Jay Aceto, CISSP, ISSAP/MP, CISM, NSA-IAM/IEM

Telephone: 571-334-9225 • E-mail Address: jay.aceto@redphonecorporation.com

Table of Contents

Executive Summary	4
Global Objectives.....	5
Penetration Testing Architecture.....	6
Findings	7
Finding No. 1: SSH	
Severity: High.....	7
Finding No. 2: SQL Injection	
Severity: Moderate.....	9
Finding No.3: Cross-site scripting (reflected)	
Severity: Moderate.....	10
Finding No.4: SSL cookie	
Severity: Low.....	11
Finding No. 5: SSL certificates	
Severity: Low.....	12
Finding No. 6: Cookie without HttpOnly flag set	
Severity: Low.....	12
Finding No. 7: Referer-dependent response	
Severity: Informational.....	13
Finding No. 8: Open redirection	
Severity: Informational.....	14
Finding No. 9: Cross-domain script include	
Severity: Informational	15
Finding No.10: Email addresses disclosed	
Severity: Informational.....	15
Finding No.10: Email addresses disclosed	
Severity: Informational.....	15
Finding No.10: Email addresses disclosed	
Severity: Informational.....	15
Finding No. 11: Robots.txt file	
Severity: Low/Informational	16
Finding No. 12: Cacheable HTTPS response	

Severity: Informational.....	17
Finding No. 13: Script files	
Severity: Moderate.....	17
Summary & Conclusions:	19

Document Properties
Title: Multi-Vendor Mock Voting Exercise – Operation Orange Black Box Penetration Testing Report
Version V1.0
Author L. Jay Aceto CISSP, CISM, ISSAP/MP, NSA-IAM/IEM
Technical Review: TC McFall
Peer Review: Josha Richards, Aaron Bossert, Michael Carter
RedPhone Penetration testers: TC McFall, L. Jay Aceto

Version control
Version : 1.0
Date : August 15, 2011

Executive Summary

The democratic process rests on a fair, universally accessible, anonymous voting system through which all citizens can easily and accurately cast their vote. At present, over 6,000,000 voters reside outside the United States and rely on traditional paper-based registration and voting processes that are inadequate at meeting their needs, and fraught with inherent delays. The main issues revolve around the inherent latency with the registration, receipt, and delivery of ballots by traditional mail. The Federal Voting Assistance Program (FVAP), a United States Department of Defense (DoD) controlled program, has been systematically gathering, analyzing, and reporting on the voter's experience, and exploring new technologies to improve the delivery of registration and ballot materials.

RedPhone, LLC., a Virginia-based information assurance and security consultancy to the U.S. DoD, civilian, and state governments, as well as commercial enterprises, was contracted to provide penetration testing services to CALIBRE Systems in support of the FVAP to test and evaluate the security of three Internet voting systems. The penetration test team was led by CALIBRE Management, however, the primary responsibility for the testing and analysis resided with RedPhone, LLC. Additionally, RedPhone, LLC. prepared the testing scenario and the rules of engagement that the Air Force Institute of Technology (AFIT) and other outside penetration testing teams would use to determine the scope and boundaries of the engagement. The fictitious *Operation Orange* exercise and the rules of engagement are listed within the appendices.

Beginning in May of 2011, and culminating in the actual penetration testing and mock election exercise that spanned 72 hours from August 2-4, 2011, all three participating vendors' systems were carefully evaluated for their security posture, defensive capabilities, critical logging and security architecture limitations. Historically, the application development processes associated with these critical applications have not followed industry best practices. This flawed state is the result of undisciplined software development, and a process that failed to encourage developers to anticipate or fix security holes. The closed-source approach to software development, which shielded the source code from public review and comment, only served to delay the necessary scrutiny. However, all three vendors have been highly supportive of these tests, and it is obvious that they have made great strides to improve the security posture of their respective products. Six independent technical security experts with an extensive background in web application security and information assurance were charged with attempting to breach the security of each of the three participating vendors. Two AFIT cyber security teams were also participating in the penetration testing process. This

report is the culmination of the penetration test team's findings, potential mitigations, and recommendations.

Penetration testing typically falls into the following three categories: "White box" testing is performed with the full knowledge and support of the vendor, and the vendor provides unlimited access to the software, supporting documentation and staff. "Grey box" testing is a partial knowledge test scenario where the test team has only limited knowledge of the vendor's products and services, and the rest must be obtained via research. In "black box" testing, the test teams are given very little if any advanced knowledge of the vendor's products, and therefore, must gain as much knowledge as possible independently in a discovery and reconnaissance effort. The penetration test team for this exercise used a "black box" approach, wherein little information is provided from the vendors, and only a brief window is available to research each vendor to prepare an attack strategy.

Although the penetration test teams designed various attacks, they generally fell into one of five categories:

1. vote manipulation at the client work station PC or server databases,
2. attacks aimed at breaking the authentication mechanism for PIN's or administrative access,
3. attacks directed at defeating voter anonymity,
4. analysis of data in transit that could have been altered, or
5. denial-of-service that prevents voters from being able to reach or cast votes.

Most attack vectors fell into the first category.

The RedPhone penetration test team applied the Open Web Application Security Project (OWASP) evaluation methodology of attack mapping, threat modeling, and poor trust relationship failure analysis to assess where to focus their attention, and then used standard pen-testing tools including attacking physical security, network scanning to locate and exploit vulnerabilities in each of the vendor system. This approach does not look at possible vulnerabilities that may be inherent in the system architecture or data handling procedures at the precinct level. Because of the very limited time and resources available, RedPhone, LLC. adopted an almost entirely ad hoc approach, focusing our attention on those parts of the system that we believed might provide the best attack vector to less secure devices within the DMZ. While we used some source code analysis tools—and several widely used "hacking" tools like Nessus, NMAP and Metasploit—we applied them only selectively, and instead adopted a more "curious" strategy most often used by an

attacker that seeks out weaknesses in the places where he would most likely find vulnerabilities, and then moving on to the next place of potential weakness. This is a very common approach used when limited time and information is available, and when known security is in place, such as out-sourced managed firewalls, routers, or intrusion detection and prevention devices. Our overall impression of the security posture for all three participating vendors was good. We did not find any significant technical security concerns, only minor correctable issues that can easily be mitigated. While time constraints were the biggest limitation, we did find at least one issues involving SSH installed on a server, presumably for remote management purposes. This was the most serious findings, as given more time, we could have likely cracked the password and gained access to the server. We found obvious places where SQL-injection exists, and were tested, but not to the extent that any were successful. Cross-site scripting (reflected) is another case wherein proper coding procedure isn't being followed; however, other mitigating security controls were in place that did not allow for successful penetration. We've documented a good number of informational findings that should be used to improve overall UOCAVA best practice security guidelines.

RedPhone wishes to emphasize that our results do not extend beyond the scope of our investigation of the technical security of the application as seen from the outside. Our scope was limited to that which is defined in our contract with CALIBBRE Systems, and do not contend that these systems are correct or secure beyond the specific findings we've addressed here. Unless otherwise noted, the results of this investigation should be assumed to be relevant only to these three vendor systems and the software version used for this test.

GLOBAL OBJECTIVES

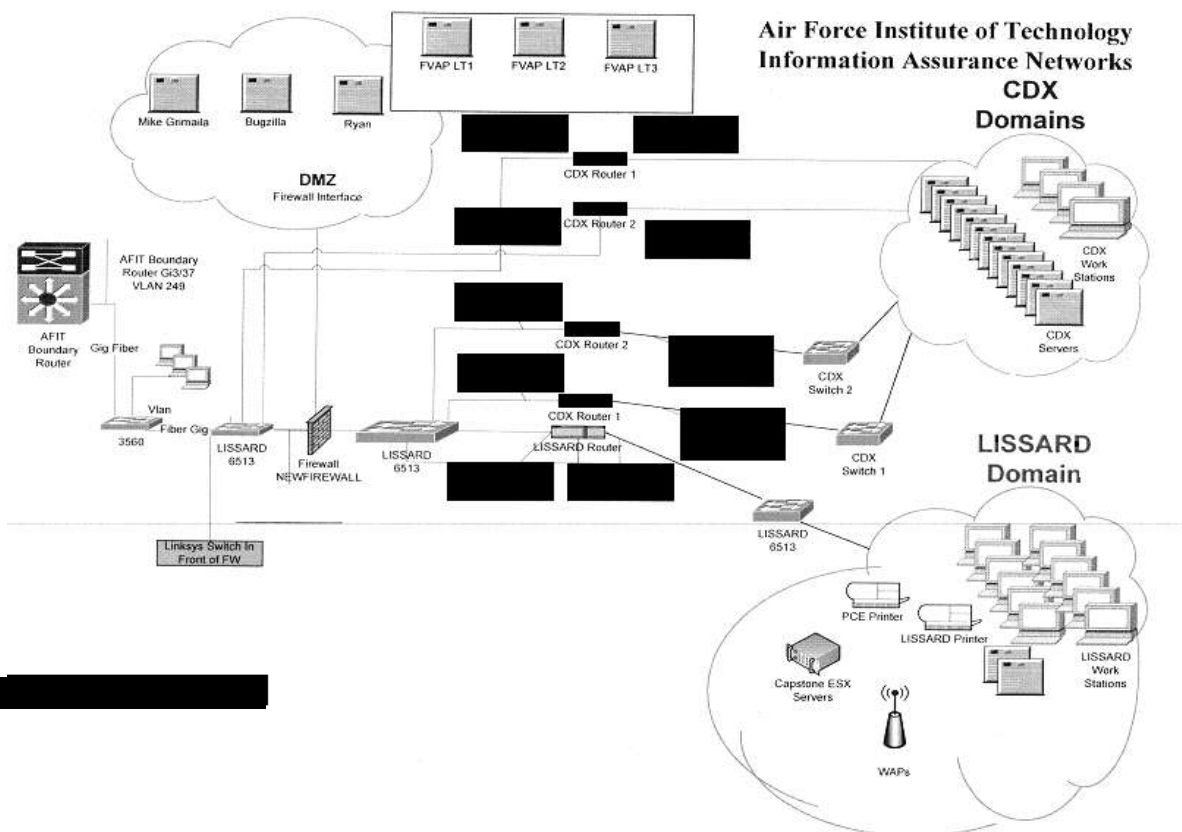
- Breach the security of each vendor's voting systems and gain access to sensitive information on the DMZ Network where a tangential attack vector could be made into the more secure voting systems.
- To emulate a realistic technical threat to the ATF computer networks from persons having no prior access or knowledge other than information that is openly available on the Internet;
- To discover and exploit any vulnerability or combination of vulnerabilities found on the system in order to meet the stated objective of the penetration test; and
- To test the extent an organization's security incident response capability is alerted and to gauge the response to such suspicious activity.

- Recommend best security practices and guidelines that would mitigate these attacks.

PENETRATION TESTING ARCHITECTURE

The AFIT network architecture used by the two internal penetration testing teams is a traditional network architecture that includes a test lab environment, routers, firewalls, a DMZ, and unfiltered access out to the Internet where the penetration test teams used MicroSoft Internet Explorer and Mozilla Firefox browsers to connect to the target servers and local workstations used as voting stations. The AFIT penetration testing team used multiple tools that included, Nessus, NMAP, Metasploit and other tools found on the BackTrack 5 live CD. A complete list of tools used by the AFIT test teams will be provided with their documentation. The RedPhone penetration team performed all their tests remotely, but was on site daily to assist with AFIT testing coordination and support. The laptops used by the AFIT teams were located with the lab environment and provided with unfiltered access to the Internet; the voting station laptops were located within the AFIT's Doolittle lounge where other Air Force personnel could use them for simulated voting. There were no physical security controls placed upon the voting work stations. Below is a high-level representation of the AFIT information assurance network used for the testing. IP addresses have been removed or blacked out.

Figure 1. AFIT Network Architecture



Findings

Each of the vendor's systems provided a level of security that was consistent with most business and technical security best practices. Each vendor's automated security systems detected our attempts to breach the security of the applications at the server side, and response and notification times were well within service level agreement time frames. Also, each vendor was able to quickly identify the attacking IP addresses, shut down the attack, and provide log verification. Therefore, we are confident that each vendor's security systems could detect and respond to most attempts to breach the security and gain access to the system. Specific technical findings are listed below:

FINDING No. 1: SSH **SEVERITY: HIGH**

Brute-force authentication attacks against one vendor's Secure Shell (SSH) service was not successful, but this service should never be made available to a production server, as penetration is almost assured given ample time.

Issue Background

US-CERT issues SSH concerns frequently and should be heeded. The SSH is a network protocol that creates a secure channel between two networked devices in order to allow data to be exchanged. SSH can create this secure channel by using Cipher Block Chaining (CBC) mode encryption. This mode adds a feedback mechanism to a block cipher that operates in a way that ensures that each block is used to modify the encryption of the next block.

SSH contains a vulnerability in the way certain types of errors are handled. Attacks leveraging this vulnerability would lead to the loss of the SSH session. According to [CPNI Vulnerability Advisory SSH](#):

If exploited, this attack can potentially allow an attacker to recover up to 32 bits of plaintext from an arbitrary block of ciphertext from a connection secured using the SSH protocol in the standard configuration. If OpenSSH is used in the standard configuration, then the attacker's success probability for recovering 32 bits of plaintext is 2^{-18} . A variant of the attack against OpenSSH in the standard configuration can verifiably recover 14 bits of plaintext with probability 2^{-14} . The success probability of the attack for other implementations of SSH is not known.

Impact

An attacker may be able to recover up to 32 bits of plaintext from an arbitrary

block of ciphertext.

Issue Mitigation

We are currently unaware of a practical solution to this problem. CERT recommends the use of CTR Mode. This mode generates the keystream by encrypting successive values of a “counter” function. For more information see the Block Cipher Modes article on wikipedia.

In order to mitigate this vulnerability, SSH can be setup to use CTR mode rather CBC mode. According to [CPNI Vulnerability Advisory SSH](#):

The most straightforward solution is to use CTR mode instead of CBC mode, since this renders SSH resistant to the attack. An RFC already exists to standardise counter mode for use in SSH (RFC 4344)...

Systems Affected

Vendor	Status	Date Notified	Date Updated
Bitvise	Vulnerable	2008-11-07	2008-11-24
FiSSH	Vulnerable	2008-11-07	2008-11-24
Icon Labs	Vulnerable	2008-11-07	2008-11-24
OpenSSH	Vulnerable	2008-11-07	2008-11-24
OSSH	Vulnerable	2008-11-07	2008-11-24
PuTTY	Vulnerable	2008-11-07	2009-01-05
Redback Networks, Inc.	Vulnerable	2008-11-07	2008-11-24
SSH Communications Security Corp	Vulnerable	2008-11-07	2008-11-24
TTSSH	Vulnerable	2008-11-07	2008-11-24
VanDyke Software	Vulnerable	2008-11-07	2009-01-12
Wind River Systems, Inc.	Vulnerable	2008-11-07	2008-11-24

References

http://www.cpni.gov.uk/Docs/Vulnerability_Advisory_SSH.txt
<http://isc.sans.org/diary.html?storyid=5366>
http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

FINDING NO. 2: SQL INJECTION

SEVERITY: MODERATE

The findings listed below are generic and do not reflect any specific vendor' s environment. We have kept them generic so that FVAP can assess the overall security posture of these voting systems and make determination about the high-level

guidance and policy recommendations that may be required.

There are five instances of this issue:

Issue background

SQL injection vulnerabilities arise when user-controllable data are incorporated into database SQL queries in an unsafe manner. An attacker can supply crafted input to break out of the data context in which their input appears and interfere with the structure of the surrounding query.

Various attacks can be delivered via SQL injection, including reading or modifying critical application data, interfering with application logic, escalating privileges within the database, and executing operating system commands.

Issue remediation

The most effective way to prevent SQL injection attacks is to use parameterised queries (also known as prepared statements) for all database access. This method uses two steps to incorporate potentially tainted data into SQL queries: first, the application specifies the structure of the query, leaving placeholders for each item of user input; second, the application specifies the contents of each placeholder. Because the structure of the query has already been defined in the first step, it is not possible for malformed data in the second step to interfere with the query structure. Documentation should be reviewed for the database and application platform to determine the appropriate APIs, which can be used to perform parameterised queries. It is strongly recommended that *every* variable data item that is incorporated into database queries is parameterised, even if it is not obviously tainted, to prevent oversights occurring and avoid vulnerabilities being introduced by changes elsewhere within the code base of the application.

FVAP should be aware that some commonly employed and recommended mitigations for SQL injection vulnerabilities are not always effective:

- One common defense is to double up any single quotation marks appearing within user input before incorporating that input into a SQL query. This defense is designed to prevent malformed data from terminating the string in which they are inserted. However, if the data being incorporated into queries are numeric, then the defense may fail, because numeric data may not be encapsulated within quotes, in which case only a space is required to break out of the data context and interfere with the query. Further, in second-order SQL injection attacks, data that has been safely escaped ("escaping" is a technique used to ensure that characters are treated as data, not as characters) when initially inserted into the database is subsequently read

from the database and then passed back to it again. Quotation marks that have been doubled up initially will return to their original form when the data are reused, allowing the defense to be bypassed.

- Another often cited defense is to use stored procedures for database access. While stored procedures can provide security benefits, they are not guaranteed to prevent SQL injection attacks. The same kinds of vulnerabilities that arise within standard dynamic SQL queries can arise if any SQL is dynamically constructed within stored procedures. Further, even if the procedure is sound, SQL injection can arise if the procedure is invoked in an unsafe manner using user-controllable data.

FINDING NO.3: CROSS-SITE SCRIPTING (REFLECTED)

SEVERITY: MODERATE

Issue detail

The value of the parenturl request parameter is copied into a JavaScript string, which is encapsulated in single quotation marks. The payload `bb8cf' %3b6b50cb864d6` was submitted in the parenturl parameter. This input was echoed as `bb8cf' ;6b50cb864d6` in the application's response.

This behavior demonstrates that it is possible to terminate the JavaScript string into which data are being copied. An attempt was made to identify a full proof-of-concept attack for injecting arbitrary JavaScript, but this was not successful. The application's behavior should be manually examined and any unusual input validation or other obstacles that may be in place should be identified.

Remediation detail

Echoing user-controllable data within a script context is inherently dangerous, and can make XSS attacks difficult to prevent. If at all possible, the application should avoid echoing user data within this context.

Issue background

Reflected cross-site scripting vulnerabilities arise when data are copied from a request and echoed into the application's immediate response in an unsafe way. An attacker can use the vulnerability to construct a request that, if issued by another application user, will cause JavaScript code supplied by the attacker to execute within the user's browser in the context of that user's session with the application.

The attacker-supplied code can perform a wide variety of actions, such as stealing

the victim' s session token or login credentials, performing arbitrary actions on the victim' s behalf, and logging their keystrokes.

Users can be induced to issue the attacker' s crafted request in various ways. For example, the attacker can send a victim a link containing a malicious URL in an email or instant message. They can submit the link to popular websites that allow content authoring, for example, in blog comments. And they can create an innocuous looking website which causes anyone viewing it to make arbitrary cross-domain requests to the vulnerable application (using either the GET or the POST method).

The security impact of cross-site scripting vulnerabilities is dependent upon the nature of the vulnerable application, the kinds of data and functionality that it contains, and the other applications that belong to the same domain and organization. If the application is used only to display non-sensitive public content, with no authentication or access control functionality, then a cross-site scripting flaw may be considered low risk. However, if the same application resides on a domain that can access cookies for other more security-critical applications, then the vulnerability could be used to attack those other applications, and so may be considered high risk. Similarly, if the organization that owns the application is a likely target for phishing attacks, then the vulnerability could be leveraged to lend credibility to such attacks by injecting Trojan functionality into the vulnerable application and exploiting users' trust in the organization in order to capture credentials for other applications that it owns. In many kinds of application, such as those providing online banking functionality, cross-site scripting should always be considered high risk.

Remediation background

In most situations where user-controllable data are copied into application responses, cross-site scripting attacks can be prevented using two layers of defenses:

- Input should be validated as strictly as possible on arrival, given the kind of content that it is expected to contain. For example, personal names should consist of alphabetical and a small range of typographical characters, and be relatively short; a year of birth should consist of exactly four numerals; email addresses should match a well-defined regular expression. Input which fails the validation should be rejected, not sanitized.
- User input should be HTML-encoded at any point where it is copied into application responses. All HTML metacharacters, including < > " ' and =, should be replaced with the corresponding HTML entities (< > etc).

In cases where the application' s functionality allows users to author content

using a restricted subset of HTML tags and attributes (for example, blog comments that allow limited formatting and linking), it is necessary to parse the supplied HTML to validate that it does not use any dangerous syntax; this is a non-trivial task.

FINDING No.4: SSL COOKIE

SEVERITY: LOW

Issue detail

The following cookie was issued by the application and does not have the secure flag set:

- `ASP.NET_SessionId=51dw1odzrv11hdjz15ztmosw; path=/; HttpOnly`

The cookie appears to contain a session token, which may increase the risk associated with this issue. The contents of the cookie should be reviewed to determine its function.

Issue background

If the secure flag is set on a cookie, then browsers will not submit the cookie in any requests that use an unencrypted HTTP connection, thereby preventing the cookie from being trivially intercepted by an attacker monitoring network traffic. If the secure flag is not set, then the cookie will be transmitted in clear-text if the user visits any HTTP URLs within the cookie's scope. An attacker may be able to induce this event by feeding a user suitable links, either directly or via another website. Even if the domain that issued the cookie does not host any content that is accessed over HTTP, an attacker may be able to use links of the form `http://example.com:443/` to perform the same attack.

Issue remediation

The secure flag should be set on all cookies that are used for transmitting sensitive data when accessing content over HTTPS. If cookies are used to transmit session tokens, then areas of the application that are accessed over HTTPS should employ their own session handling mechanism and the session tokens used should never be transmitted over unencrypted communications.

FINDING No. 5: SSL CERTIFICATES

SEVERITY: LOW

This finding is more informational than an actual vulnerability. The vendor had "self-signed" the certificate, and therefore, would not be a trusted certificate, but the vendor had brought this to our attention and explained that this would not be the norm. The other two vendors had implemented the use of certificates

properly.

Issue background

SSL helps to protect the confidentiality and integrity of information in transit between the browser and server, and to provide authentication of the server's identity. To serve this purpose, the server must: present an SSL certificate that is valid for the server's hostname, is issued by a trusted authority and is valid for the current date. If any one of these requirements is not met, SSL connections to the server will not provide the full protection for which SSL is designed.

It should be noted that various attacks exist against SSL in general, and in the context of HTTPS web connections. It may be possible for a determined and suitably-positioned attacker to compromise SSL connections without user detection even when a valid SSL certificate is used.

FINDING NO. 6: COOKIE WITHOUT HTTPONLY FLAG SET

SEVERITY: LOW

This is mostly informational but does constitute a concern.

Issue detail

The following cookie was issued by the application and does not have the HttpOnly flag set:

- JSESSIONID=AB6295DFFAFA6F01E835E88C50F597ED; Path=/portal-webapp; Secure

The cookie appears to contain a session token, which may increase the risk associated with this issue. The contents of the cookie should be reviewed to determine its function.

Issue background

If the HttpOnly attribute is set on a cookie, then the cookie's value cannot be read or set by client-side JavaScript. This measure can prevent certain client-side attacks, such as cross-site scripting, from trivially capturing the cookie's value via an injected script.

Issue remediation

There is usually no good reason not to set the HttpOnly flag on all cookies. Unless legitimate client-side scripts are specifically required within an application to read or set a cookie's value, the HttpOnly flag should be set by including this attribute within the relevant Set-cookie directive.

Guidance should make implementers aware that the restrictions imposed by the

HttpOnly flag can potentially be circumvented in some circumstances, and that numerous other serious attacks can be delivered by client-side script injection, aside from simple cookie stealing.

FINDING NO. 7: REFERER-DEPENDENT RESPONSE

SEVERITY: INFORMATIONAL

Issue description

The application's responses appear to depend systematically on the presence or absence of the Referer header in requests. This behavior does not necessarily constitute a security vulnerability, and the nature of and reason for the differential responses should be investigated to determine whether a vulnerability is present.

Common explanations for Referer-dependent responses include:

- Referer-based access controls, where the application assumes that if the user has arrived from one privileged location then he/she is authorized to access another privileged location. These controls can be trivially defeated by supplying an accepted Referer header in requests for the vulnerable function.
- Attempts to prevent cross-site request forgery attacks by verifying that requests to perform privileged actions originated from within the application itself and not from some external location. Such defenses are not robust—methods have existed through which an attacker can forge or mask the Referer header contained within a target user's requests by leveraging client-side technologies such as Flash and other techniques.
- Delivery of Referer-tailored content, such as welcome messages to visitors from specific domains, search-engine optimisation (SEO) techniques, and other ways of tailoring the user's experience. Such behaviors often have no security impact, however, unsafe processing of the Referer header may introduce vulnerabilities such as SQL injection and cross-site scripting. If parts of the document (such as META keywords) are updated based on search engine queries contained in the Referer header, then the application may be vulnerable to persistent code injection attacks, in which search terms are manipulated to cause malicious content to appear in responses served to other application users.

Issue remediation

The Referer header is not a robust foundation on which to build any security measures, such as access controls or defenses against cross-site request forgery. Any such measures should be replaced with more secure alternatives that are not

vulnerable to Referer spoofing.

If the contents of responses is updated based on Referer data, then the same defenses against malicious input should be employed here as for any other kinds of user-supplied data.

FINDING No. 8: OPEN REDIRECTION

SEVERITY: INFORMATIONAL

Issue detail

The value of the Referer HTTP header is used to perform an HTTP redirect. The payload `//acec8732e3c7ad76d/a%3fhhttp%3a//www.google.com/search%3fh1%3den%26q%3d` was submitted in the Referer HTTP header. This caused a redirection to the following URL:

- `//acec8732e3c7ad76d/a%3fhhttp%3a//www.google.com/search%3fh1%3den%26q%3d`

The application attempts to prevent redirection attacks by blocking absolute redirection targets starting with `http://` or `https://`. However, an attacker can defeat this defense by omitting the protocol prefix from their absolute URL. If a redirection target starting with `//` is specified, then the browser will use the same protocol as the page that issued the redirection.

Because the data used in the redirection are submitted within a header, the application's behavior is unlikely to be directly useful in lending credibility to a phishing attack. This limitation considerably mitigates the impact of the vulnerability.

Remediation detail

When attempting to block absolute redirection targets, the application should verify that the target begins with a single slash followed by a letter and should reject any input containing a sequence of two slash characters.

Issue background

Open redirection vulnerabilities arise when an application incorporates user-controllable data into the target of a redirection in an unsafe way. An attacker can construct a URL within the application, which causes a redirection to an arbitrary external domain. This behavior can be leveraged to facilitate phishing attacks against users of the application. The ability to use an authentic application URL, targeting the correct domain with a valid SSL certificate (if SSL is used), lends credibility to the phishing attack because many users, even if they verify these features, will not notice the subsequent redirection to a different

domain.

Remediation background

If possible, applications should avoid incorporating user-controllable data into redirection targets. In many cases, this behavior can be avoided in two ways:

- Remove the redirection function from the application, and replace links to it with direct links to the relevant target URLs.
- Maintain a server-side list of all URLs that are permitted for redirection. Instead of passing the target URL as a parameter to the redirector, pass an index into this list.

If it is considered unavoidable for the redirection function to receive user-controllable input and incorporate this into the redirection target. One of the following measures should be used to minimize the risk of redirection attacks:

- The application should use relative URLs in all of its redirects, and the redirection function should strictly validate that the URL received is a relative URL.
- The application should use URLs relative to the web root for all of its redirects, and the redirection function should validate that the URL received starts with a slash character. It should then prepend `http://yourdomainname.com` to the URL before issuing the redirect.
- The application should use absolute URLs for all of its redirects, and the redirection function should verify that the user-supplied URL begins with `http://yourdomainname.com/` before issuing the redirect.

FINDING NO. 9: CROSS-DOMAIN SCRIPT INCLUDE SEVERITY: INFORMATIONAL

Issue detail

The response dynamically includes the following script from another domain:

- `https://seal.verisign.com/getseal?host_name=www.intvoting.com&size=S&use_flash=NO&use_transparent=NO&lang=en`

Issue background

When an application includes a script from an external domain, this script is executed by the browser within the security context of the invoking application. The script can therefore do anything that the application's own scripts can do,

such as accessing application data and performing actions within the context of the current user.

If a script from an external domain is included, then that domain is trusted with the data and functionality of your application, and the domain's own security to prevent an attacker from modifying the script to perform malicious actions within your application.

Issue remediation

Scripts should not be included from untrusted domains. If there is a requirement that a third-party script appears to fulfill, then ideally the contents of that script should be copied onto your own domain and include it from there. If that is not possible (e.g., for licensing reasons), then re-implementing the script's functionality within your own code should be considered.

FINDING No.10: EMAIL ADDRESSES DISCLOSED

SEVERITY: INFORMATIONAL

Issue detail

During the discovery and reconnaissance phase, we found many vendor email addresses were available. Caution should be taken to train all employees of spear phishing attacks. Spear phishing describes any highly targeted phishing attack. Spear phishers send e-mail that appears genuine to some or all the employees or members within a certain company, government agency, organization, or group. The message might look like it comes from your employer, or from a colleague sending an e-mail message to everyone in the company (such as the person who manages the computer systems) and could include requests for user names or passwords.

The truth is that the e-mail sender information has been faked or "spoofed." Whereas traditional phishing scams are designed to steal information from individuals, spear phishing scams work to gain access to a company's entire computer system. If an employee responds with a user name or password, or if click links or open attachments in a spear phishing e-mail, pop-up window, or website, he/she might become a victim of identity theft and might put his/her employer or group at risk.

Spear phishing also describes scams that target people who use a certain product or website. Scam artists use any information they can to personalize a phishing scam to as specific a group as possible.

Issue background

The presence of email addresses within application responses does not necessarily constitute a security vulnerability. Email addresses may appear intentionally within contact information, and many applications (such as web mail) include arbitrary third-party email addresses within their core content.

However, email addresses of developers and other individuals (whether appearing on-

screen or hidden within page source) may disclose information that is useful to an attacker; for example, they may represent usernames that can be used at the application's login, and they may be used in social engineering attacks against the organization's personnel. Unnecessary or excessive disclosure of email addresses may also lead to an increase in the volume of spam email received.

Issue remediation

FVAP should review and offer guidance concerning the email addresses being disclosed by the application, and consider removing any that are unnecessary, or replacing personal addresses with anonymous mailbox addresses (such as helpdesk@example.com).

FINDING NO. 11: ROBOTS.TXT FILE

SEVERITY: LOW/INFORMATIONAL

While this issue can often give away information to an attacker, this particular instance did not. Therefore, this is informational only.

Issue detail

The web server contains a robots.txt file.

Issue background

The file robots.txt is used to give instructions to web robots, such as search engine crawlers, about locations within the website that robots are allowed, or not allowed, to crawl and index.

The presence of the robots.txt does not in itself present any kind of security vulnerability. However, it is often used to identify restricted or private areas of a site's contents. The information in the file may, therefore, help an attacker to map out the site's contents, especially if some of the locations identified are not linked from elsewhere in the site. If the application relies on robots.txt to protect access to these areas and does not enforce proper access control over them, then this presents a serious vulnerability.

Issue remediation

The robots.txt file is not itself a security threat, and its correct use can represent good practice for non-security reasons. You should not assume that all web robots will honor the file's instructions. Rather, assume that attackers will pay close attention to any locations identified in the file. Do not rely on robots.txt to provide any kind of protection over unauthorized access.

FINDING No. 12: CACHEABLE HTTPS RESPONSE

SEVERITY: INFORMATIONAL

There are three instances of this issue. This is a minor issue, bordering on informational. These are the result of implementation errors that can be easily corrected.

Issue description

Unless directed otherwise, browsers may store a local cached copy of content received from web servers. Some browsers, including Internet Explorer, cache content accessed via HTTPS. If sensitive information in application responses is stored in the local cache, then this may be retrieved by other users who have access to the same computer at a future time.

Issue remediation

The application should return caching directives instructing browsers not to store local copies of any sensitive data. Often, this can be achieved by configuring the web server to prevent caching for relevant paths within the web root.

Alternatively, most web development platforms allow control of the server's caching directives from within individual scripts. Ideally, the web server should return the following HTTP headers in all responses containing sensitive content:

- Cache-control: no-store
- Pragma: no-cache

FINDING No. 13: SCRIPT FILES

SEVERITY: MODERATE

We successfully downloaded all site scripts from every vendor, no exceptions. With more time allotted to a penetration, this would be a severe issue. Going through the script's contents (and comment sections, etc.) would allow for detailed mapping of site functionality. Hardening of application server configurations is highly recommended for each vendor, in order to mitigate this threat.

Additional tests performed

These types of Distributed Denial-of-Service (DDoS) attacks are not new. Organizations have been battling them since they became popular in the late 1990s. While techniques to defend against DDoS attacks have become more sophisticated, they still represent a difficult challenge and major risk. Limited Denial-of-Service (DoS) attacks were performed. These were unsuccessful. However, mention should be given that no DDoS attacks were performed due to lack of

resources available for the test. It is entirely feasible for a mass denial attack to be successful, and this is an eventuality that is difficult to mitigate.

The DoS attack is focused on making unavailable a resource (site, application, server) for the purpose it was designed. There are many ways to make a service unavailable for legitimate users by manipulating network packets, programming, logical, or resources handling vulnerabilities, among others. If a service receives a very large number of requests, it may stop providing service to legitimate users. In the same way, a service may stop if a programming vulnerability is exploited.

Sometimes the attacker can inject and execute arbitrary code while performing a DoS attack in order to access critical information or execute commands on the server. DoS attacks significantly degrade service quality experienced by legitimate users. It introduces large response delays, excessive losses, and service interruptions, resulting in direct impact on availability.

DoS & DDoS Locking Customer Accounts

The first DoS case to consider involves the authentication system of the target application. A common defense to prevent brute-force discovery of user passwords is to lock an account from use after between three to five failed attempts to login. This means that even if a legitimate user were to provide their valid password, they would be unable to login to the system until their account has been unlocked. This defense mechanism can be turned into a DoS attack against an application if there is a way to predict valid login accounts.

Note: there is a business vs. security balance that must be reached based on the specific circumstances surrounding a given application. There are pros and cons to locking accounts, to customers being able to choose their own account names, to using systems such as CAPTCHA, and the like. Each enterprise will need to balance these risks and benefits, but not all of the details of those decisions are covered here. It should be noted that one vendor does incorporate CAPTCHA as a deterrent to this form of attack. Specific controls to combat DDoS attacks can include:

1. working with the Internet Service Provider (ISP) to establish quality of service rates to limit the amount of bandwidth one customer can utilize;
2. using firewalls and filtering devices to filter all unnecessary ports and protocols;
3. incorporating redundancy and resiliency into designs of key systems; and
4. utilizing IDS/IPS to identify and block attacks in progress

Related Attacks

- Resource Injection
- Setting Manipulation
- Regular expression Denial of Service - ReDoS

Related Vulnerabilities

- Category: Input Validation Vulnerability
- Category: API Abuse

Summary & Conclusions:

Internet based voting systems should be certified and recertified on a regular basis since changes to the operating systems, applications, services, protocols etc. change frequently. All defensive strategies should be risk-based and right-sized to match the risk. In a perfect world, every company could employ every defense possible to protect against every type of attack on every part of its infrastructure. In reality, however, time and resources are not unlimited. Defenses have to be selected and deployed based on a cost-benefit methodology. Voting systems face unique threats, some are at the nation-state level, and therefore, unlimited resources, and game changing technologies could be leveraged to crash services, corrupt votes via insider threats, or devise methods to social engineer perceptions causing voter disenfranchisement. The controls must be appropriate to the risks.

RedPhone suggests that the FVAP determine what department within the federal government is responsible for determining threats associated with the voting process so that an appropriate risk assessment can be done based on known threats. FVAP should use formal risk analysis and cost-benefit analysis to help ensure their control environment is appropriate for their risk profile and tolerance. The risk analysis should include several key steps.

First, the FVAP should perform a formal risk analysis to determine the actual risk to the environment. The risk assessment should consider the value of the assets being protected, likelihood of probable threats and attack vectors, impact of a successful attack, inherent risk of the condition, existing safeguards, and the residual risk as compared to current tolerance.

Next, based on the results of the risk assessment, determine what areas of the voting process are operating at unacceptable levels of risk. Identify controls that can reduce the likelihood of the threat source or lessen the impact to acceptable levels. Perform a cost-benefit analysis to determine if the suggested controls provide an appropriate risk reduction benefit.

The next step should be to implement appropriate controls based on this analysis. Test the controls and likely attack scenarios to validate the controls operate properly and provide the desired effect. Employ monitoring, metrics and measures to ensure key controls continue to perform adequately and provide the expected protections. Continually update the risk assessment as new threats emerge, the business makes changes or other factors change that would affect the risk assessment results. The risk assessment should be updated at least annually to ensure it is still appropriate for the organization and the current environment.

It should be noted that this test had several limitations that would not exist in the “real world”, and therefore additional testing is highly recommended. Also, it should be noted that all testing is a “point-in-time-analysis”, and therefore should never be considered lasting. Testing should be performed with some regularity to maintain the highest level of security posture at all times.

Operational policies for high confidentiality, integrity and availability focus on setting and establishing processes, policies, and strict configuration and patch management. They are divided into the following categories:

- Service Level Management for High Availability
- Planning Capacity to Promote High Availability
- Change Management for High Availability
- Backup and Recovery Planning for High Availability
- Disaster Recovery Planning
- Planning Scheduled Outages
- Staff Training for High Availability
- Documentation as a Means of Maintaining High Availability
- Physical Security Policies and Procedures for High Availability

In addition to the above policies, a well defined and documented software development life-cycle should be adopted. The Capability Maturity Model Integration (CMMI) is a widely followed and adopted best practice that defines practices that include eliciting and managing requirements, decision making, measuring performance, planning work, handling risks, and more. None of the vendors' voting systems are being developed using such a defined life-cycle. We recommend that voting systems vendors adopt rigorous software engineering practices based on CMMI level-3 or better to ensure that system life-cycle, documentation, and methodologies are not random, but instead meet or exceed best practices.

The single greatest risk to Internet voting from an end-users computer is the fact that election officials do not have access to the voting workstation to determine its integrity, nor the upstream Internet supporting infrastructure. However, if a kiosk approach is employed, the election officials still have some control over the environment; it is recommended that the kiosk periodically send "status votes" or "test ballots" that test the integrity and accuracy of the voting system and the end-to-end transmission of the encrypted data. Control of the client-side voting computer, the local network, or upstream Internet Service Providers (ISP's) infrastructure will always present significant challenges to Internet based voting. Therefore, it is imperative that both end-points, and the lines of communication be as secure as possible to maintain the vote integrity, confidentiality, system availability and voter anonymity.

Appendix – C Operation Orange

Jonathan Wright is a tall, handsome, slightly exotic looking Harvard grad, who has served in the U.S. Senate for 8 years. He has recently won the appointment as a candidate for the office of the President of the United States. He has the backing of the military and firefighters of America, as well as various police districts. However, unbeknownst to most of the American public is the fact that though he was born in the U.S., Senator Wright's grandfather, still resides in this fictional nation state.

Now, this nation state is very interested in the latest election because the incumbent president of the U.S. is considering a boycott of all CFS light bulbs, a major product for this nation state. For years they have been the only manufacturers of this product; however, the light bulbs often have defects that have caused severe injuries to American consumers—leading to a public outcry against the product. American and Mexican companies are now producing a superior, if more expensive, light bulb.

Because this issue is in the fore front of the American psyche, the incumbent president wants it to be one of the issues of his platform. A boycott of this product would be a devastating financial blow to their economy. This nation state requires a president sympathetic to their cause in the oval office.

Mr. Wright will champion the product over an American or Mexican one. Primarily, because Mr. Wright still has close family that resides in this nation state; and therefore, he should honor the family name as a proud descendant. This nation state government believes that Mr. Wright would want to support his family's home nation, and maintain their status has the premier supplier of CFS light bulbs. Therefore, this nation state is confident that they will be able to hack the American electronic voting systems to ensure Mr. Wright's election to the office of president.

Specific Objectives:

Acting as hackers, your objective is to hack into the voting system, obtain administrator level rights and access, and *change* the votes so that Senator Wright becomes the next president of the United States. You must “recon” the targeted electronic voting system(s) and thoroughly plan your plan of attack employing sophisticated penetration techniques. If the changes are detected and an audit deems hacking has altered the targeted system(s), the election will merely be deemed void or corrupt and a new one will take place using old fashioned methods beyond the control of the nation state. Furthermore, you must do your best to cover

your “tracks” such that cyber security personnel will not be able to forensically trace the hack to your IP address.

You will have a limited amount of time to perform your reconnaissance of the vendor system(s), determine what tools to use, and ultimately penetrate the system(s) and make the needed changes to ensure the desired outcome. A denial of service attack would quickly be detected and traced, therefore this method of disruption should not be considered.

Keeping in mind that these penetration tests are intended to provide the following:

- Evaluate the protection of the Vendor’ s electronic voting systems with a special emphasis on the effectiveness of logical access and system software security controls
 - Provide value to the Vendor’ s electronic voting system by identifying opportunities to significantly strengthen applicable controls within budgetary and operational constraints
- i.e., documented mitigation strategies, or security patches and/or procedures that improve the security posture of their respective systems.
- To facilitate timely, cost-effective completion of this project, Tiger Teams will make maximum practical use of the relevant work of others where possible (i.e., internal assessments by the auditee, internal and external audits, and vulnerability testing on covered IT assets).
 - In order to optimize the effectiveness of the Penetration Test team members, the Vendor’ s need to provide access to systems, services, and employees. To perform the work specified in this statement of work, the Tiger Teams will require the following from the customer:
 1. Access to relevant personnel including: technical support, data center personnel, application developers and end-users and functional experts.
 2. Relevant documentation including: System Administration Guides, System Architecture diagrams that include IP addresses of target systems. Previous security threat assessments if available.
 3. A primary point of contact for emergency remediation if needed.
 4. Coordination of events with customer team members.

5. Signed NDA, Authorization to Proceed, and the below Rules of Engagement.

Appendix – D Tools

Information Gatheringbr	Assbr	DMitrybr	DNS-Ptrbr	dnswalkbr
dns-bruteforcebr	dnsenumbr	dnsmapbr	DNSPredictbr	Finger Googlebr
Firewalkbr	Goog Mail Enumbr	Google-searchbr	Goograpebr	Gooscanbr
Hostbr	ltracebr	Netenumbr	Netmaskbr	Piranabr
Protosbr	QGooglebr	Relay Scannerbr	SMTP-Vrfybr	TCtracebr
Network Mappingbr	Amap br	Assbr	Autoscan _Rbr	Fpingbr
Hpingbr	IKE-Scanbr	IKEProbebr	Netdiscoverbr	Nmapbr
NmapFEbr	Pfbr	PSK-Crackbr	Pingbr	Protosbr
Scanrandbr	SinFPbr	Umitbr	UnicornScanbr	UnicornScan pgsql e
module version br	Analysisbr br	Servicesbr	SNORTp	SIPcrackbr
XProbebr	PBNJ br	OutputPBNJbr	ScanPBNJbr	Genlistbr
Vulnerability Identificationbr	Absinthebr	Bedbr	CIRT Fuzzerbr	Checkpwdbr
Cisco Auditing Toolbr	Cisco Enable Bruteforcerbr	Cisco Global Exploiterbr	Cisco OCS Mass Scannerbr	Cisco Scannerbr
Cisco Torchbr	Curlbr	Fuzzer br	GFI LanGuard br	GetSidsbr
HTTP PUTbr	Halberdbr	Httpprintbr	Httpprint GUIbr	ISR-Formbr
Jbrofuzzbr	List-Urlsbr	Lynxbr	Merge Router Configbr	Metacoretexbr
Metoscanbr	Mezcal HTTPSbr	Mibble MIB Browserbr	Mistressbr	Niktobr
OATbr	Onesixtyonebr	OpenSSL-Scannerbr	Paros Proxybr	Peachbr
RPCDumpbr	RevHostsbr	SMB Bruteforcerbr	SMB Clientbr	SMB Serverscanbr
SMB-NATbr	SMBdumpusersbr	SMBgetserverinfobr	SNMP Scannerbr	SNMP Walkbr
SQL Injectbr	SQL Scannerbr	SQLLibfbr	SQLbrutebr	Sidguessbr
SmbKbr	Snmpcheckbr	Snmp Enumbr	Spikebr	Stompybr
SuperScanbr	TNScmdbr	Taofbr	VNC_bypauthbr	Wapitibr
Yersiniabr	sqlanzbr	sqldictbr	sqldumploginsbr	sqlquerybr
sqluploadbr	Penetrationbr	Framework-MsfCbr	Framework-MsfUpdatebr	Framework-Msfclib
Framework-Msfwebbr	Init Pgsq (autopwn)br	MilwrM Archivebr	MsfClibr	MsfConsolebr
MsfUpdatebr	OpenSSL-To-Openbr	Update MilwrMbr	Privilege Escalationbr	Ascend attackerbr
CDP Spooferbr	Cisco Enable Bruteforcerbr	Crunch Dictgenbr	DHCPX Flooderbr	DNSspooferbr
Driftnetbr	Dsniffbr	Etherapebr	EtterCapbr	FileCablebr
HSRP Spooferbr	Hash Collisionbr	Httpcapturebr	Hydrabr	Hydra GTKbr
ICMP Redirectbr	ICMPushbr	IGRP Spooferbr	IRDP Responderbr	IRDP Spooferbr
Johnbr	Lodoweprbr	Mailsnarfbr	Medusabr	Msgsnarfbr
Nemesis Spooferbr	NetSedbr	Netenumbr	Netmaskbr	Ntopbr
PHossbr	PackETHbr	Rcrackbr	SIPdumpbr	SMB Snifferbr
Singbr	TFTP-Brutebr	THC PPTPbr	TcPickbr	URLsnarfbr
VNCCrackbr	WebCrackbr	Wiresharkbr	Wireshark Wifibr	WyDbr
XSpybr	chntpwbr	Maintaining Accessbr	proxybr	Backdoorsbr
CryptCatbr	HttpTunnel Clientbr	HttpTunnel Serverbr	ICMPTXbr	Iodinebr
NSTXbr	Privoxybr	ProxyTunnelbr	Rinetdbr	TinyProxybr
sbdbr	socatbr	Covering Tracksbr	Housekeepingbr	Radio Network
Replaybr	AFragbr	ASLeapbr	Air Crackbr	Air Decapbr Air
	Airmon Scriptbr	Airpwnbr	AirSnarfbr	Airodumpbr
	Hexdumpbr			
Airoscripbr	Airsnortbr	CowPattybr	FakeAPbr	GenKeysbr
Genpmkbr	Hotspotterbr	Karmabr	Kismetbr	Load IPWbr
Load acxbr	MDKbr	MDK for Broadcombr	MacChangerbr	Unload Driversbr
Wep_crackbr	Wep_decryptbr	WifiTapbr	Wicrawlbr	Wlassistantbr
Bluetoothbr	Bluebuggerbr	Blueprintbr	Bluesnarferbr	Btscannerbr
Carwhispererbr	CuteCombr	Ghettotoothbr	HCIDumpbr	Ussp-Pushbr
OllyDBGbr	PcapSipDumpbr	PcapToSip RTPbr	SIPSakbr	Hexeditbr
SIPdumpbr	SIPpbr	Smabr	Digital Forensicsbr	Allinbr
Autopsybr	DCFLDDbr	DD_Rescuebr	Foremostbr	Magicrescuebr
Mboxgrepbr	Memfetchbr	Memfetch Findbr	Pascobr	Rootkithunterbr

Sleuthkit
GDB Server

Vinetto
GNU DDD

Reverse Engineering
VOIP & Telephony Analysis

GDB GNU Debugger

GDB Console GUI



Because of some last minute corrections to the ROE/MNDA/ATS documentation, we requested email confirmation of the acceptance. Those e-mail acceptances are below:

From Vendor-2.com
to Jay Aceto <jay.aceto@redphonecorporation.com>
date Sat, Jul 30, 2011 at 9:35 PM
subject RE: Error found. Please resign ROE' s & Authorizations
to Scan ASAP
Important mainly because it was sent directly to you.

Jay,

On behalf of Vendor-2 I accept the changed documents. I will bring signed copies Monday.

Vice President
Vendor-2

from @Vendor-3.com
to Jay Aceto <jay.aceto@redphonecorporation.com>
date Mon, Aug 1, 2011 at 9:51 AM
subject RE: Error found. Please resign ROE's & Authorizations to Scan ASAP
mailed-by Vendor-3.com

Jay,

I accept the corrections on behalf of Vendor-3.

Vendor-3

From: Vendor-1.com>
To: "Jay Aceto (jay.aceto@redphonecorporation.com)"
<jay.aceto@redphonecorporation.com>
Date: Fri, 22 Jul 2011 15:58:37 -0700
Subject: Student Forms

Hi Jay,

Attached are our authorization signatures and Rules of Engagements for the students...

Vendor-1, Inc.

Appendix C

Federal Voting Assistance Program (FVAP) Security Gap Analysis of UOCAVA Pilot Program Testing Requirements

8 February 2011



Security Gap Analysis of UOCAVA Pilot Program Testing Requirements

Delivery Order CT 80047-0037

Task 5.1.3

FINAL Report

February 8, 2011

Executive Summary

A complete Internet voting system could provide voter identification and authentication, voter registration, election administration, ballot delivery, voting, tabulation, and results reporting. However, any such electronic voting (eVoting) system must be able to insure privacy and security to the voting individual, as well as confirmation of their vote. However, there are many federal information systems that provide secure data transfer of privacy information and data of higher national security that are arguably far more sensitive than voting information that are currently in use and have met the requirements of the most stringent security guidance.

In December 2010, CALIBRE cyber security subject matter experts (SMEs) reached out to industry and federal agency contacts for additional insights on threats capable of launching a successful distributed denial of service (DDoS) attack or exploiting vulnerabilities associated with an eVoting system. A call for recommendations and insights was sent to senior cyber security experts and national security advisors. Additionally, CALIBRE contacted Carnegie Mellon University's Software Engineering Institute and Computer Emergency Response Team (CERT) for additional recommendations.

Simultaneously, CALIBRE began base-lining current UOCAVA testing requirements to determine if they meet current cyber threats. In total, 259 requirements were identified in the UOCAVA Pilot Program Test document from August 2008–2010. While many are functional requirements, all were evaluated for their security risk and potential exploit impacts. A security matrix was used to map the requirements to multiple industry and federal government security best practices and mandated requirements including: The National Institute of Standards and Technology (NIST), The International Standards Organization (ISO), Federal Information Security Management Act (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).

Of the 259 requirements identified and evaluated, some only impact one of the three areas (confidentiality, integrity and availability), but others could impact more than one. One hundred fifty requirements impacted confidentiality, 246 impacted integrity, and 191 impacted availability. Of the 259 requirements, only 41 were categorized as having a low impact to security. However, 130 were considered to have a medium impact, and 88 were considered to have a high potential impact.

Of the 259 identified UOCAVA Pilot Program Testing Requirements, 186 meet specific federal guidance in the seven documents and are listed as “compliant” in the security requirements traceability matrix. Of the 259 requirements, 30 could not be traced directly to a federal requirement in the seven identified guidance documents. Therefore, it was unknown whether these requirements meet technical security requirements. Fifteen of the requirements are functional and do not have a security impact, and thereby, do not need to be reconciled. However, reconciliation with federal or international standards of 15 requirements was recommended. CALIBRE attempted to locate all documents listed as references within the UOCAVA Pilot Program Testing Requirements to match the 15 to possible requirements listed in those references. Not all of the references were located. However, of the un-reconciled 15 UOCAVA

Pilot Program Testing Requirements only 2 were found within the located references and were reconciled. Of the 13 requirements that were not found, they *do* follow best business practices.

Fifty-eight requirements were identified as functional (including the 15 mentioned above) and had no direct impact on security; they are only a functionality of the voting system. The most relevant finding is that NONE of the requirements that were traced were identified as NOT being compliant with the guidance, i.e., there are no notable gaps between UOCAVA Pilot Program Testing Requirements and the security guidance of the seven documents used in this analysis.

Table of Contents

Executive Summaryiii

Table of Tablesvi

1 Background 7

2 Scope..... 8

3 Methodology 9

 3.1 Identification of Mission and Data Classification..... 9

 3.1.1 The Mission of FVAP 9

 3.1.2 Selection of MAC I and Confidentiality Level Sensitive..... 9

 3.1.3 Relevant Government Guidances..... 10

 3.1.4 Industry/Federal Data Call 11

 3.1.5 Internet Search 12

4 Technical Gap Analysis 13

5 Recommendations..... **Error! Bookmark not defined.**

Appendix A Security Requirements Traceability Matrix 27

Appendix B References..... 28

Appendix C Glossary 32

Table of Tables

Table 1. Applicable IA Controls by MAC and CL Level 10

Table 2. Referenced Guidance 13

Table 3. Operating Environment Summary by Confidentiality Level According to NIST 15

Table 4. Operating Environment Summary by Confidentiality Level According to DIACAP 16

Table 5. Operating Environment Summary by Confidentiality Level According to DCID 6/3 17

Table 6. Recommendations to the UOCAVA Pilot Program Testing Requirements 19

Table 7. UOCAVA Pilot Program Testing Requirements that are not reconciled with guidance 21

Table 8. UOCAVA Security Control Reconciliation..... 22

1 Background

The Federal Voting Assistance Program (FVAP) administers the federal responsibilities of the Presidential designee (Secretary of Defense) under the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) of 1986. The Director, FVAP administers the Act on behalf of the Secretary of Defense.

The Act covers more than six million potential voters including the following:

- Active duty members of the uniformed services including the Coast Guard, commissioned corps of the Public Health Services, the Merchant Marine, and National Oceanic and Atmosphere Administration (NOAA);
- Their voting age dependents; and
- U.S. citizens residing outside the United States.

A complete electronic voting (eVoting) system would provide voter identification and authentication, voter registration, election administration, ballot delivery, voting, tabulation, and results reporting. However, any such eVoting system must be able to insure privacy and security to the voting individual, as well as confirmation of their vote.

2 Scope

The CALIBRE team, in support of FVAP efforts to develop the most secure remote voting capabilities, has been contracted to provide a technical gap analysis of testing procedures and related policies. In accordance with established guidance, [including NIST's research on security issues associated with remote electronic UOCAVA voting, and in coordination with the FVAP Office, the Wounded Warrior Care and Transition Policy (WWCTP) Office, and the Election Assistance Commission (EAC)] the CALIBRE team will conduct a variety of research, analysis, evaluation, and gap mitigation strategies to meet FVAP's strategic goals. The primary intent is to improve the policies, processes, and procedures for Wounded Warriors, disabled military members, military members, their dependents, and overseas civilian voters to register and vote successfully and securely with a minimum amount of effort.

3 Methodology

During the months of December 2010 and January 2011, a policy analysis team assembled relevant UOCAVA and FVAP materials and reviewed all known security-related concerns and policies relative to the UOCAVA Pilot Program Testing Requirements to understand these security issues. These efforts included, but were not limited, to the following:

- Identify all currently available UOCAVA, EAC, and FVAP mission and confidentiality policies.
- Identify mission assurance and confidentiality levels.
- Identify most appropriate federal and industry best practices and guidance. Perform line-at-a-time comparison of UOCAVA Program Testing Requirements to all the chosen federally recognized and supported guidance standards.
- Produce a gap analysis and correlate identified security weaknesses with national vulnerability databases.
- Provide analysis of results.
- Identify mitigating methodologies and approaches when possible.

3.1 Identification of Mission and Data Classification

3.1.1 The Mission of FVAP

FVAP's mission is to facilitate the absentee voting process for UOCAVA citizens living around the world. This includes: consulting with state and local election officials; prescribing the Federal Post Card Application (FPCA) for absentee registration/ballot requests, along with Federal Write-in Absentee Ballots (FWAB); and distributing descriptive material on state absentee registration and voting procedures. FVAP has three primary focus areas within its mission:

- Assist military and overseas voters in exercising their right to vote.
- Assist state and local election officials in complying with the requirements of federal law, and in providing equal voting opportunity for military and overseas voters.
- Advocate for military and overseas voting rights with federal, state and local governments.

3.1.2 Selection of MAC I and Confidentiality Level Sensitive

It is difficult to assign a DoD Mission Assurance Category (MAC) to the e-Voting system. However, in DoD Directive 8500.1 (Information Assurance) the DoD defines Mission Assurance Category I (MAC I) as the following: "Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include

the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.”¹

While MAC I relates only to deployed forces outside the continental U.S. (OCONUS) and information that can affect their mission effectiveness, because the electoral process is considered to be an issue of national security, the e-Voting system would fall within this MAC level.

As for the confidentiality level (CL)² of the e-Voting system, the data stored in the system most closely matches the definition of sensitive data. For reasons of national security and for the highest level of confidentiality appropriate to the electoral process, we are evaluating the systems based on this level of classified.

Therefore, our analysis of the UOCAVA Pilot Program Testing Requirements in relation to the e-Voting system has been assigned the highest level Mission Assurance Category of I and confidentiality level of Classified, and will be evaluated against those Information Assurance (IA) controls.

Table 1. Applicable IA Controls by MAC and CL Level

Mission Assurance Category and Confidentiality Level	Applicable IA Controls
MAC I, Classified	Encl. 4, Attachments A1 (Mission Assurance Category I Controls for Integrity and Availability) and A4 (Confidentiality Controls for DoD Information Systems Processing Classified Information)
MAC I, Sensitive	Encl. 4, Attachments A1 and A5
MAC I, Public	Encl. 4, Attachments A1 and A6
MAC II, Classified	Encl. 4, Attachments A2 and A4
MAC II, Sensitive	Encl. 4, Attachments A2 and A5
MAC II, Public	Encl. 4, Attachments A3 and A6
MAC III, Classified	Encl. 4, Attachments A3 and A4
MAC III, Sensitive	Encl. 4, Attachments A3 and A5
MAC III, Public	Encl. 4, Attachments A3 and A6

3.1.3 Relevant Government Guidance

The UOCAVA Pilot Program Testing Requirements were derived from 120 references. These references range from a “Request for Proposal” and the Nevada Gaming Commission and State Gaming Control Board to IEEE standards³. While a few NIST special publications are listed, there are no references to current DIACAP guidance—which is needed for certification and accreditation if FVAP requires

¹ <http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf>

² <http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf>, Table E4.T3. Operating Environment Summary by Confidentiality Levels

³ UOCAVA Pilot Program Testing Requirements, Appendix B.

certification and accreditation (C&A). Of the 259 identified requirements, 99 are security specific (only 32 percent). While UOCAVA made a significant effort to capture and define requirements based on 100-plus seemingly relevant guidance, we believe that fewer, more succinct references will benefit FVAP in the technical gap analysis.

Therefore, CALIBRE used seven prevailing IA documents for the Pilot Program Testing Requirements technical gap analysis. Within the Information Assurance industry there are multiple documents that provide guidance to civilian agencies, DoD and the intelligence community. For the civilian agencies, the dominant guiding documents are the NIST Special Publications; for DoD, there is the DIACAP guidance⁴; and for the intelligence community, there is the DCID 6/3. These three prevailing guidance documents are used to support this technical gap analysis for the following reasons. FVAP is a DoD entity, and therefore, falls under DIACAP processes. FVAP has a mission to support both DoD and civilian overseas personnel; falling under the NIST guidelines. However, because the electoral process is considered to be an issue of national security, the DCID 6/3 guidance must also be considered in the technical gap analysis.

In addition to this guidance, CALIBRE also referenced ISO 17799 (the International Standards Organization) due to the international requirements of FVAP, and ICD 503 (Intelligence Community Directive)—which was to replace DIACAP¹ in the analysis. FISMA guidance⁵ and Government Accounting Office (GAO) FISCAM guidance⁶ were also used because they are the mandating documents guiding all IA requirements within the U.S. Government.

3.1.4 Industry/Federal Data Call

In addition to the UOCAVA Pilot Testing Program gap analysis, CALIBRE has reached out to industry and federal agency contacts for additional insights on threats capable of launching a successful distributed denial of service (DDoS) attack on an election system. A data call for recommendations and insights were sent to 12 senior cyber security experts and national security advisors. Carnegie Mellon University's Software Engineering Institute and Computer Emergency Response Team (CERT) were contacted for additional guidance and recommendations. Aaron Bossert, a senior software exploit analyst for CERT has recommended that FVAP require vendors to apply the NIST SP-800-137 methodology and tools to the development and implementation of eVoting software. The recently developed NIST Software Assurance Metrics and Tool Evaluation (SAMATE) project defines software assurance as a "planned and systematic" set of activities that ensures that software processes and products conform to requirements, standards and procedures from the NASA Software Assurance Guidebook and Standard to better achieve the following:

- Trustworthiness—no exploitable vulnerabilities exist, either of malicious or unintentional origin (i.e., nothing is transmitted externally that will put the system at risk.)

⁴ DIACAP guidance was intended to be replaced by Intelligence Community Directive (ICD503). However, this transition has not been widely adopted.

⁵ The Federal Information Security Management Act of 2002.

⁶ GAO Federal Information System Controls Audit Manual (FISCAM), 2009.

- Predictable Execution—justifiable confidence that software, when executed, functions as intended.

3.1.5 Internet Search

CALIBRE searched the following international vulnerability databases for technical vulnerabilities associated with the UOCAVA Pilot Program Testing Requirements:

- Microsoft Technical Databases
- NIST National Vulnerability Database
- National Checklist Program (automatable security configuration guidance in XCCDF & OVAL)
- SCAP (program and protocol that NVD supports)
- SCAP Compatible Tools
- SCAP Data Feeds (CVE, CCE, CPE, CVSS, XCCDF, OVAL)
- Product Dictionary (CPE)
- Impact Metrics (CVSS)
- Common Weakness Enumeration (CWE)
- CVE Vulnerabilities—<http://cve.mitre.org/>
- Checklists—<http://web.nvd.nist.gov/view/ncp/repository>
- US-CERT Alerts—<http://www.us-cert.gov/cas/techalerts/>
- US-CERT Vuln Notes— <http://www.kb.cert.org/vuls/byupdate?open&start=1&count=10>
- OVAL Queries—<http://oval.mitre.org/>
- Secunia—<http://secunia.com/advisories/search/>
- packetstorm— <http://packetstormsecurity.org/files/tags/exploit/>
- SANS Internet storm center— <http://isc.incidents.org/>
- OSVDB—http://osvdb.org/project_aims

4 Technical Gap Analysis

CALIBRE performed a technical gap analysis to compare existing UOCAVA internally published testing requirements with multiple federally supported and industry recognized information assurance guidance. The results were then compared to determine the current protection posture specific to e-Voting in order to better understand how effective those policies and requirements were in meeting security needs for eVoting as defined in the current government and industry standards.

This technical gap analysis identifies gaps in the current UOCAVA Pilot Program Testing Requirements (August 2008) based on guidance from multiple sources. The most widely referenced information assurance guidance comes from the following federally supported documents:

Table 2. Referenced Guidance

Selected Guidance	Summary
The National Institute of Standards and Technology (NIST) Special Publications Series SP800-53A Rev2.	NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Management Act (FISMA) of 2002 and in managing cost-effective programs to protect their information and information systems.
The International Standards Organizations (ISO) and the International ElectroTechnical Commission (IEC)	<p>ISO/IEC 17799:2005 is a code improved protection of practice for information security management.</p> <p>The revised ISO/IEC 17799:2005 is the most important standard for managing information security that has been developed.</p>
The Government Accounting Office (GAO) Federal Information System Control Audit Manual (FISCAM)	<p>Provides security requirements for applicable controls specific to the applications they support. However, they generally involve ensuring that:</p> <ul style="list-style-type: none"> - data prepared for entry are complete, valid, and reliable; - data are converted to an automated form and entered into the application accurately, completely, and on time; - data are processed by the application completely and on time, and in accordance with established requirements; and - output is protected from unauthorized modification or damage and distributed in accordance with prescribed policies.

Selected Guidance	Summary
The FIPS199/200	<p>Standards to be used by all federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels.</p> <p>Guidelines recommending the types of information and information systems to be included in each category.</p> <p>Minimum information security requirements (i.e., management, operational, and technical controls) for information and information systems in each such category.</p> <p>Standards for categorizing information and information systems collected or maintained by or on behalf of each federal agency based on the objective of providing appropriate levels of information security according to a range of risk levels.</p> <p>Guidelines recommending the types of information and information systems to be included in each category.</p> <p>Minimum information security requirements for information and information systems in each such category.</p>
The Department of Defense 8500.2	Implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks.
The Director Central Intelligence Directive 6/3	<p>Provides uniform policy guidance and requirements for ensuring adequate protection of certain categories of intelligence information;</p> <p>Provides guidance to assist an Information System Security Manager (ISSM) or Information System Security Officer/Network Security Officer, (ISSO/NSO) in structuring and implementing the security protections for a system.</p>
Intelligence Community Directive 503 (ICD 503)	ICD focuses on a holistic and strategic process for the risk management of information technology systems, and on processes and procedures designed to develop the use of common standards across the intelligence community.

CALIBRE created a baseline of current UOCAVA Testing Requirements to determine if they meet current cyber threats. In total, 259 requirements were identified in the UOCAVA Pilot Program Test document from August 2008–2010. While many are functional requirements, all were evaluated for their security risk and potential exploit impacts. Using the NIST guidance, DIACAP guidance and DCID 6/3, the impacts were

rated as low, medium and high relative to confidentiality, integrity, and availability. The definition of the categories as stated by the three guidance methodologies is shown in the following tables.

Table 3. Operating Environment Summary by Confidentiality Level According to NIST

Security Objective	Potential Impact		
	Low	Medium	High
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction; includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. Basic Testing: A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object.	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Table 4. Operating Environment Summary by Confidentiality Level According to DIACAP

Confidentiality Level	Internal System Exposure	External System Exposure
High (Systems Processing Classified Information)	<ul style="list-style-type: none"> • Each user has a clearance for all information processed, stored or transmitted by the system. • Each user has access approval for all information stored or transmitted by the system. • Each user is granted access only to information for which the user has a valid need-to-know. 	<ul style="list-style-type: none"> • System complies with DoDD C-5200.5 reference (aj) requirements for physical or cryptographic isolation. • All Internet access is prohibited. • All enclave interconnections with enclaves in the same security domain require boundary protection (e.g., firewalls, IDS, and a DMZ). • All enclave interconnections with enclaves in a different security domain require a controlled interface. • All interconnections undergo a security review and approval.
Medium (Systems Processing Sensitive Information)	<ul style="list-style-type: none"> • Each user has access approval for all information stored or transmitted by the system. • Each user is granted access only to information for which the user has a valid need-to-know. • Each IT user meets security criteria commensurate with the duties of the position. 	<ul style="list-style-type: none"> • All non-DoD network access (e.g., Internet) is managed through a central access point with boundary protections (e.g., a DMZ). • All enclave interconnections with enclaves in the same security domain require boundary protection (e.g., firewalls, IDS, and a DMZ). • All remote user access is managed through a central access point. • All interconnections undergo a security review and approval.
Basic (Systems Processing Public Information)	<ul style="list-style-type: none"> • Each user has access approval for all information stored or transmitted by the system. • Each IT user meets security criteria commensurate with the duties of the position. 	<ul style="list-style-type: none"> • N/A as the purpose of system is providing publicly released information to the public.

Table 5. Operating Environment Summary by Confidentiality Level According to DCID 6/3⁷

Level of Concern	Confidentiality Indicators (Chapter 4)	Integrity Indicators (Chapter 5)	
Basic	Not applicable to this manual.	Reasonable degree of resistance required against unauthorized modification; or loss of integrity will have an adverse effect.	
Medium	Not applicable to this manual.	High degree of resistance required against unauthorized modification; or bodily injury might result from loss of integrity; or loss of integrity will have an adverse effect on organizational-level interests.	
High	All Information Protecting Intelligence Sources, Methods and Analytical Procedures. All Sensitive Compartmented Information.	Very high degree of resistance required against unauthorized modification; or loss of life might result from loss of integrity; or loss of integrity will have an adverse effect on national-level interests; or loss of integrity will have an adverse effect on confidentiality.	
Protection Levels According to DCID 6/3			
Lowest Clearance	Formal Access Approval	Need To Know	Protection Level
At Least Equal to Highest Data	All Users Have ALL	All Users Have ALL	1 (paragraph 4.B.1)
At Least Equal to Highest Data	All Users Have ALL	NOT ALL Users Have ALL	2 (paragraph 4.B.2)
At Least Equal to Highest Data	NOT ALL users have ALL	Not Contributing to Decision	3 (paragraph 4.B.3)
Secret	Not Contributing to Decision	Not Contributing to Decision	4 (paragraph 4.B.4)
Un-cleared	Not Contributing to Decision	Not Contributing to Decision	5 (paragraph 4.B.5)

There are no additional security requirements under the DCID 6/3 guidance, and the translation of the confidentiality, integrity and availability is directed at secure compartmented information (SCI) and the need to know. We've taken the high water mark of a High PL1 DCID 6/3 security profile for the UOCAVA Pilot Program Testing gap analysis.

A Pilot Program Testing Requirements Matrix⁸ was created to map the requirements to multiple industry and federal government security best practices and mandated requirements as identified in Table 2.

We searched for security weaknesses and gaps by associating UOCAVA Pilot Program Testing Requirements with the seven guidance documents. Of the 259 requirements identified and evaluated, some only impact one of the three areas (confidentiality, integrity and availability), but others could impact more than one; 150 requirements impacted confidentiality, 246 impacted integrity, and 191

⁷ Director Central Intelligence Directive 6/3, http://www.fas.org/irp/offdocs/DCID_6-3_20Manual.htm#Protection Levels

⁸ See Appendix A: Security Requirements Traceability Matrix

impacted availability. Of the 259 requirements, only 41 were categorized as having a low impact to security. However, 130 were considered to have a medium impact, and 88 were considered to have a high potential impact.

Of the 259 identified UOCAVA Pilot Program Testing Requirements, 186 meet specific federal guidance in the seven documents and are listed as “compliant” in the security requirements traceability matrix. Of the 259 requirements, 30 could not be traced directly to a federal requirement in the seven identified guidance documents. Therefore, it was unknown whether these requirements meet technical security requirements. Fifteen of the requirements are functional and do not have a security impact, and thereby, do not need to be reconciled. However, reconciliation with federal or international standards of 15 requirements was recommended. CALIBRE attempted to locate all documents listed as references within the UOCAVA Pilot Program Testing Requirements to match the 15 to possible requirements listed in those references. Not all of the references were located. However, of the un-reconciled 15 UOCAVA Pilot Program Testing Requirements only 2 were found within the located references and were reconciled. Of the 13 requirements that were not found, they *do* follow best business practices.

Fifty-eight requirements were identified as functional (including the 15 mentioned above), and had no direct impact on security; they are only a functionality of the voting system. The most relevant finding is that NONE of the requirements that were traced were identified as NOT being compliant with the guidance, i.e., there are no notable gaps between UOCAVA Pilot Program Testing Requirements and the security guidance of the seven documents used in this analysis.

5 Recommendations

The industry assumption is that technology is a step behind the high level of encryption. This assumption, however, is continually challenged by advances in technology. For FVAP, the challenges are further complicated by the fact that the majority of sophisticated and well-funded threat information is held in a classified status and is not available for general disclosure. Furthermore, in the computer world, information a month old is often outdated. The most recent publication, the *NIST Draft White Paper on Security Considerations for Remote Electronic UOCAVA Voting* (which is still out for comments), documents threats to UOCAVA voting systems using electronic technologies for overseas and military voting. However, by the time it is formally released, the cyber threat community may have ensured that the information is no longer viable.

Therefore, once the new security requirements have been identified and/or mitigated, they should be tracked over time to address changes in regulatory compliance, new attack vectors, threats and known vulnerabilities; the weighing of effort required to protect vulnerabilities will need to be assessed frequently as new technologies and exploit capabilities are developed or become known.

5.1 Recommendations to the UOCAVA Pilot Program Testing Requirements

CALIBRE recommends that FVAP address the following areas based on identified potential technical vulnerabilities and security weaknesses within the UOCAVA Pilot Program Testing Requirements. (See Table 6).

Table 6. Recommendations to the UOCAVA Pilot Program Testing Requirements

Item	UOCAVA Req. No.	Recommendations
1.	2.2.3	Recommend that the following guidance be referenced and followed. NIST SP800-52 provides guidance on protecting transmission integrity using TLS. Other NIST documents include SP800-81, 800-44, 800-45, 800-49, 800-57, 800-58, 800-66, 800-77 and 800-81. FIPS 198 also discusses transmission quality.
2.	2.3.1.1	Recommend that all graphic file formats be tested for corruption from malformed packets. Known vulnerabilities exist with almost all graphic file formats. Appropriate patches to operating systems must be tested.
3.	2.3.1.2	No recommendation. However, the requirement does not specify how this is to be accomplished.
4.	2.6.2.2	See recommendation for 2.3.1.1.
5.	2.6.2.3	See recommendation for 2.3.1.1.
6.	2.7.1.1	Recommend that IDS/IPS system(s) SHALL be used that actively monitors, detects, and notifies system administrators of any potential malicious activity.
7.	4.9.1.3	Recommend the use of application scanning tools such as Fortify 360, Nessus,

Item	UOCAVA Req. No.	Recommendations
		Lumension etc. to identify source code vulnerabilities.
8.	4.9.1.4	See recommendation for 4.9.1.3.
9.	5.1.1.1	See recommendation for 4.9.1.3.
10.	5.1.1.2	See recommendation for 4.9.1.3.
11.	5.2.1.1	Recommend the use of three-factor authentication method to include biometric with a Cross over Error Rates (CER) and Equal Error Rates that meet minimum DoD requirements.
12.	5.2.1.3	Recommend that passwords conform to DOD minimum requirements.
13.	5.2.1.12	Recommend that authentication schema SHALL be commensurate with the highest level technically feasible, as this will constantly change as new schemas become available.
14.	5.3.1.2	See recommendation for 5.2.1.12.
15.	9.5.1.9	Recommend adoption of DoD guidance for erasable media.

The following table is a list of UOCAVA Pilot Program Testing Requirements that were not found in any of the seven governmental guidance documents used for the technical gap analysis. The requirements on this list should be reconciled. (See Table 7).

Table 7. UOCAVA Pilot Program Testing Requirements that are Not Reconciled with Guidances.

Item	UOCAVA Requirement Number	UOCAVA Requirement Title
1.	4.3.1.2	Module Testability
2.	4.3.1.3	Module Size and Identification
3.	4.7.2.7	Nullify Freed Pointers
4.	4.7.2.8	Do not disable error checks
5.	4.7.2.11	Election Integrity Monitoring
6.	5.4.1.2	Cast Vote Integrity Storage
7.	5.4.1.3	Cast Vote Storage
8.	5.4.1.4	Electronic Ballot Box Integrity
9.	6.2	Components from Third Parties
10.	6.3	Responsibilities for Tests
11.	7.5.2	Function Configuration Audit (FCA)
12.	8.2.1	TDP Implementation
13.	8.3.4.1	Hardwired and Mechanical implementations of logic
14.	8.3.4.2	Logic Specifications for PLD's, FPGA's and PIC's
15.	8.4.5.3	Justify Coding Conventions
16.	8.4.6.1	Application Logic Operating Environment
17.	8.4.7.1	Hardware Environment and Constraints
18.	8.4.8.2	Compilers and Assemblers
19.	8.4.8.3	Interpreters
20.	8.4.9.1	Application logic functional specification
21.	9.2.3.3	Traceability of Procured Software
22.	9.4.5.1	Ballot Count and Vote Total Auditing
23.	9.5.1.4	Election Specific Software Identification
24.	9.5.1.7	Compiler Installation Prohibited

Item	UOCAVA Requirement Number	UOCAVA Requirement Title
25.	9.5.1.8	Procurement of System Software
26.	9.6.1.2	Setup Inspection Record generation
27.	9.6.1.12	Consumables quantity of vote capture device
28.	9.6.1.13	Consumables Inspection Procedures
29.	9.6.1.14	Calibration of vote capture devices components nominal range
30.	9.6.1.15	Calibration of vote capture device components inspection procedure

At this point, CALIBRE researched the UOCAVA Pilot Program Testing Requirements references to attempt to map the 30 un-reconciled requirements to other guidance. Of the 30 requirements to be reconciled, 15 were functional and did not have a security impact, and 2 were found in other related federal references. The remaining 13 requirements could not be mapped to specific federal regulatory guidance or requirements, but do support best business practices. (See Table 8.)

Table. 8 UOCAVA Security Control Reconciliation

UOCAVA Requirement	Impact (C,I,A)	Risk	Comment
4.7.2.7 Nullify Freed Pointers	I, A	Medium	A best coding practice. Recommend that coding follow CMMI level-3 methodologies at a minimum.
6.3 Responsibility for tests	I, A	Medium	No specific regulatory requirement for manufactures to perform tests. Normally included within the RFP.
8.3.4.1 Hardwired and mechanical implementation logic	C, I, A	High	Falls under border logic. This should be addressed within the System Security Plan.
8.3.4.2 Logic specification for PLD's, FPGA's, and PIC's	C, I, A	High	Falls under border logic. This should be addressed within the System Security Plan.
8.4.5.3 Justify coding conventions	C, I, A	Medium	No specific regulation identified. Can be addressed within the RFP.
8.4.8.3 Interpreters	C, I, A	Low	No specific NIST or IEEE Requirements identified for COTS runtime code version. However, this should be documented within the System Security Plan.
8.4.9.1 Application logic functional specifications	C, I, A	Low	No specific NIST or IEEE Requirements identified for COTS runtime code version. However, this should be documented within the System Security Plan.
9.5.1.4 Election specific software identification	I	Medium	This is best security practice, but no specific federal regulatory reference could be identified.
9.5.1.7 Compiler installation prohibited	C, I, A	Medium	This is best security practice, but no specific federal regulatory reference could be identified.
9.6.1.2 Setup inspection record generation	C, I, A	Medium	Ref. in NIST SP800-100 speaks to security checklists. Should be addressed within the System Security Plan.
9.6.1.12 Consumables quantity of vote capture device	A	Low	Not a significant risk.
9.6.1.13 Consumables inspection	A	Low	No specific security risk. Mentioned in NIST H143 and media

UOCAVA Requirement	Impact (C,I,A)	Risk	Comment
procedures			storage. Should be addressed within the System Security Plan.
9.6.1.14 Calibration of vote capture device components nominal range	I	Medium	This should fall under System Security Plan guidance. Should be addressed within the System Security Plan.

Note: for column 2, C=Confidentiality, I=Integrity, and A=Availability.

5.2 Things to Consider

5.2.1 Software Monitoring

Our data call research indicates that several automation specifications exist to support the continuous monitoring of software assurance, including the emerging Software Assurance Automation Protocol (SwAAP) that is being developed to measure and evaluate software weaknesses and assurance cases. SwAAP uses a variety of automation specifications such as the Common Weakness Enumeration (CWE), which is a dictionary of weaknesses that can lead to exploitable vulnerabilities, and the Common Weakness Scoring System (CWSS) for assigning risk scores to weaknesses. SwAAP also uses the Common Attack Pattern Enumeration & Classification (CAPEC)—which is a publicly available catalog of attack patterns with a comprehensive schema and classification taxonomy—to provide descriptions of common methods for exploiting software, and the Malware Attribute Enumeration & Characterization (MAEC), which provides a standardized language for encoding and communicating information about malware based upon attributes such as behaviors, artifacts, and attack patterns.

5.2.2 Other Secure Systems

There are many federal information systems that provide secure data transfer of privacy information and data of higher national security that are arguably far more sensitive than voting information and are currently in use and have met the requirements of the most stringent security guidance. For example, the EQIP⁹ and JPAS¹⁰ systems have been online for quite some time, and one can draw some very important parallels to an e-Voting system. They have to support the reality that a user may access it from any internet-connected computer system, and they must verify the relative security of that system. Another parallel is that the sensitivity is arguably equal to or greater than an e-Voting system.

Furthermore, the IRS uses the Electronic Federal Tax Payment System (EFTPS). Tax returns contain considerable privacy information including: name, address, rank, SSN, income, income sources, deductions, dependents, donations, and investments. However, since 1986, and with over 400 million

⁹ EQIP is the Office of Personnel Management's background investigation tool. It has a diagnostic tool for evaluating the security of a PC to determine if it meets security requirements. This could also be used for remote voting via Internet.

¹⁰ <http://www.dss.mil/diss/jpas/jpas.html>

returns, the IRS e-file system has never been compromised. According to the IRS website, the following facts and information are true.

- *The IRS e-file System is not done over e-mail.*
- *The IRS e-file System has many built-in security features.*
- *The IRS e-file System employs multiple firewalls.*
- *The IRS e-file System uses state of the art virus and worm detection.*
- *The IRS e-file System meets or exceeds all government security standards.*
- *The IRS e-file System is constantly tested for weaknesses by penetration testing.*
- *The IRS e-file System has never had a security breach.*
- *All Internet transmissions will use SSL (Secure Sockets Layer) encrypted security measures.*

IRS e-file transmissions are very secure because the IRS has been extremely diligent in the design, development, analysis and testing of the current infrastructure and system. IRS e-file meets or exceeds all government security standards and includes multiple firewalls.

Most e-filed online tax returns are transmitted over phone lines from the return preparer to a third-party transmitter. From there, the returns are forwarded over secured lines to the IRS. Intercepting telephone transmissions is quite difficult and requires access to phone company major transmission lines. Also, to transmit data like tax returns over telecommunications lines means that the information gets converted into digital format, which could not be easily read even if it were intercepted.¹¹

Because user confidence and demand is high, the IRS has recently designed and deployed a mobile application for use across inherently unsecured wireless connection (e.g., iPhone/Android apps).

In addition to these federally supported, secure online capabilities, financial institutions and stock trading companies (such as eTrade), as well as many healthcare institutions are heavily dependent upon transfer of privacy based data that supports extremely high system availability and data integrity. All of these systems must be compliant with federal guidance. If EQIP, JPAS and these others were certified and accredited and are in use today, then certainly a similar approach and technology could be taken when considering what risks are acceptable in an e-Voting system.

There is yet another consideration—even though there was a valiant effort made to document the risks associated with the current overseas voting system, and a hypothetical electronic system has been discussed, it is very important to make a direct comparison between the current threats to the existing system and the equivalent threats to a proposed electronic system, such as:

- The current paper-based system is susceptible to “man-in-the-middle” attacks with little or no mechanisms in place to detect or prevent them.
- Personal information (PII) can be stolen elsewhere and can be used to forge ballots.

¹¹ <http://www.irs.gov/efile/article/0,,id=121477,00.html>

- Physical signatures are less secure than properly implemented digital ones when it is considered that even though one can reliably verify that a physical signature is authentic, it is rarely done due to being prohibitively expensive to implement on this scale.
- This e-Voting system is no more, or less susceptible to DDoS or other types of attack than any other system; as such it could take advantage of the very well accepted countermeasures to these types of attacks. (Recently, DDoS attacks directed at WikiLeaks during the Cablegate scandal proved to be relatively ineffective, and WikiLeaks dealt with the attack quickly.)

While there are some serious security vulnerabilities that need to be addressed in terms of e-Voting, it is not impossible to implement a sufficiently secure e-Voting system, assuming that the cost of the countermeasures is acceptable.

Appendix A Security Requirements Traceability Matrix



FVAP_UOCAVA_SRT
M_v16.xls

Appendix A can be found on pg. 706 of this document

Appendix B References

1. Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), (as modified by the National Defense Authorization Act for FY 2005). <http://www.fvap.gov/resources/media/uocavalaw.pdf>
2. 107th U.S. Congress (October 29, 2002). "Help America Vote Act of 2002 (Pub. L. 107-252)." U.S. Government Printing Office.
3. National Institute of Standards and Technology Interagency Report: 7551, *A Threat Analysis on UOCAVA Voting Systems*, December 2008.
4. Draft National Institute of Standards and Technology Interagency Report 7682, *Information System Security Best Practices for UOCAVA Supporting Systems*, April 2010.
5. U.S. Election Assistance Commission (March 24, 2010). UOCAVA Pilot Program Testing Requirements, March 24, 2010. Accessed May 10, 2010 at <http://www.eac.gov/program-areas/voting-systems/docs/requirements-03-24-10-uocava-pilot-program>
6. EAC (2010, April 26). Report to Congress on EAC's Efforts to Establish Guidelines for Remote Electronic Absentee Voting Systems. Accessed May 10, 2010 at <http://www.eac.gov/program-areas/voting-systems/docs/04-26-10-move-act-report-to-congress-final-congress/>
7. M. Volkamer and R. Vogt. Basic set of security requirements for Online Voting Products. Common Criteria Protection Profile BSI-CC-PP-0037, Bundesamt für Sicherheit in der Informationstechnik, Bonn, April 2008.
8. Council of Europe. Legal, Operational, and Technical Standards for E-Voting. Recommendation Rec (2004)11, September 2004.
9. Federal Voting Assistance Program. *Secure Electronic Registration and Voting Experiment. Threat Risk Assessment- Phase 3*. March 23, 2004.
10. McConnell, Steven (2004), *Code Complete* (Second Edition), Microsoft Press.
11. Georgia Tech Information Security Center (2008). *Emerging Cyber Threats Report for 2009*. Accessed May 15, 2010 at <http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf>
12. US-CERT (2008, May 16). *Technical Cyber Security Alert TA08-137A: Debian/Ubuntu OpenSSL Random Number Generator Vulnerability*. Accessed May 15, 2010 at <http://www.us-cert.gov/cas/techalerts/TA08-137A.html>
13. Symantec (2010, April). *Symantec Global Internet Security Threat Report: Trends for 2009*. Accessed May 15, 2010 at http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf
14. Dierks, T. and Rescorla, E., *The TLS Protocol Version 1.2*, Internet Engineering Task Force, Request for Comment 5246, August 2008, <http://tools.ietf.org/html/rfc5246>

15. Atsushi Fujioka, Tatsuaki Okamoto, and Kazui Ohta. A Practical Secret Voting Scheme for Large Scale Elections. In Jennifer Seberry and Yuliang Zheng, editors, *Advances in Cryptology - AUSCRYPT '92*, volume 718 of *Lecture Notes in Computer Science*, pages 244--251, Berlin, 1993. Springer-Verlag.
16. Rene Peralta. Issues, non-issues and cryptographic tools for Internet-based voting. In *Secure Electronic Voting* (Boston, 2003), Dimitris A. Gritzalis, editor. Kluwer Academic Publishers, pp. 153-164.
17. Lorrie Faith Cranor and Ron K. Cytron, Sensus: A Security-Conscious Electronic Polling System for the Internet. *Proceedings of the Hawai'i International Conference on System Sciences*, January 7-10, 1997, Wailea, Hawaii, USA.
18. J. Benaloh and D. Tuinstra. Receipt-Free Secret-Ballot Elections. *Proceedings of the 26th ACM Symposium on Theory of Computing*. Montreal, PQ. May 1994. (New York, USA: ACM 1994), pp. 544—553.
19. Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. *A secure and optimally efficient multi-authority election scheme*. European Transactions on Telecommunications, 8:481-489, 1997.
20. Premiere Election Solutions (2008, August 19). *Product Advisory Notice*. Accessed May 15, 2010 at <http://www.sos.state.oh.us/sos/upload/news/20081001c.pdf>
21. Fink, R.A.; Sherman, A.T.; Carback, R.; , "TPM Meets DRE: Reducing the Trust Base for Electronic Voting Using Trusted Platform Modules," *Information Forensics and Security, IEEE Transactions on* , vol.4, no.4, pp.628-637, Dec. 2009.
22. Ben Adida, Olivier de Marneffe, Olivier Pereira, and Jean-Jacques Quisquater. Electing a University President Using Open-Audit Voting: Analysis of Real-World Use of Helios, In D. Jefferson, J.L. Hall, T. Moran, editor(s), *Electronic Voting Technology Workshop/Workshop on Trustworthy Elections*, Usenix, August 2009.
23. Nathanael Paul, Andrew S. Tanenbaum, "The Design of a Trustworthy Voting System," Computer Security Applications Conference, Annual, pp. 507-517, 2009 Annual Computer Security Applications Conference, 2009.
24. Common Criteria for Information Security Evaluation. Part 3: Security assurance components. Version 3.1, Rev. 3, July 2009.
25. Patrick Peterson, Henry Stern. "Botnets Gone Wild! Captured, Observed, Unraveled, Exterminated." Presented at RSA 2010, San Francisco, CA, March 1-5, 2010.
26. Testimony of Bob Carey, Director of FVAP. (2010) EAC Public Meeting, Dec. 3 2009. Accessed April 5, 2010 at http://www.eac.gov/public_meeting_12032010/
27. United States Postal Service (2007). *2007 Comprehensive Statement*. Accessed March 17, 2010 at http://www.usps.com/strategicplanning/cs07/chpt5_001.htm

28. Alvarez, R. Michael (2005, October 5). "Precinct Voting Denial of Service", *NIST Threats to Voting Systems Workshop*. Accessed March 17, 2010 at http://vote.nist.gov/threats/papers/precinct_dos.pdf
29. Davis, Joshua (2007, August 21). "Hackers Take Down the Most Wired Country in Europe" *Wired Magazine*. Accessed March 5, 2010 at http://www.wired.com/politics/security/magazine/15-09/ff_estonia
30. Markoff, John (2008, August 13). "Before the Gunfire, Cyberattacks" *The New York Times*. Accessed March 5, 2010 at <http://www.nytimes.com/2008/08/13/technology/13cyber.html>
31. Vixie, Paul, Sneeringer, Gerry, and Mark Schleifer (2002, November 24). Events of 21-Oct-2002." Accessed March 5, 2010 at <http://d.root-servers.org/october21.txt>
32. Internet Corporation for Assigned Names and Numbers. "Factsheet- Root server attack on 6 February 2007." Accessed March 5, 2010 at <http://www.icann.org/announcements/factsheet-dns-attack-08mar07.pdf>
33. Worthham, Jenna, and Andrew E. Kramer (2009, August 7) "Professor Main Target of Assault on Twitter" *The New York Times*. Accessed March 5, 2010 at <http://www.nytimes.com/2009/08/08/technology/internet/08twitter.html>
34. D. J. Bernstein and Eric Schenk (1996). *SYN Cookies*. 1996. Accessed May 15, 2010 at <http://cr.yp.to/syncookies.html>
35. Mell, Peter and Tim Grance (2009, October 7), *The NIST Definition of Cloud Computing*. Accessed March 2, 2010 at <http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc>
36. U.S. Election Assistance Commission (2006, December). *Election Crimes: An Initial Review and Recommendations for Future Study*. Accessed June 15, 2010 at http://www.eac.gov/assets/1/workflow_staging/Page/57.PDF
37. Gartner (2009, April 14). *Gartner Says Number of Phishing Attacks on U.S. Consumers Increased 40 Percent in 2008*. Accessed March 5, 2010 at <http://www.gartner.com/it/page.jsp?id=936913>
38. Cormac Herley and Dinei Florencio, A Profitless Endeavor: Phishing as Tragedy of the Commons, in *Proc. New Security Paradigms Workshop*, Association for Computing Machinery, Inc., September 2008.
39. Anti-Phishing Working Group (2009). *Phishing Activity Trends Report, 4th Quarter 2009*. Accessed March 5, 2010 at http://www.antiphishing.org/reports/apwg_report_Q4_2009.pdf
40. Office of Management and Budget (2006, June 23). *OMB Memo M06-16*. Accessed March 5, 2010 at <http://www.whitehouse.gov/OMB/memoranda/fy2006/m06-16.pdf>
41. McAfee Labs (2009). *2010 Threat Predictions*. Accessed April 13, 2010 at http://www.mcafee.com/us/local_content/white_papers/7985rpt_labs_threat_predict_1209_v2.pdf
42. Department of Defense. *Common Access Card*. Accessed March 5, 2010 at <http://www.cac.mil/>

43. National Institute of Standards and Technology (2009). *About Personal Identity Verification (PIV) of Federal Employees and Contractors*. Accessed March 5, 2010 at <http://csrc.nist.gov/groups/SNS/piv/>
44. Estonian National Electoral Committee. *Internet voting in Estonia*. Accessed March 5, 2010 at http://www.vvk.ee/public/dok/Internet_Voting_in_Estonia.pdf
45. Mozilla Foundation (2006, November 14). *Firefox 2 Phishing Protection Effectiveness Testing*. Accessed April 5, 2010 at <http://www.mozilla.org/security/phishing-test.html>
46. S. Egelman, L. Cranor, and J. Hong. You've Been Warned: An Empirical Study on the Effectiveness of Web Browser Phishing Warnings. CHI '08: Proceedings of the SIGCHI conference on Human Factors in Computing Systems. April 2008.
47. National Institute of Standards and Technology (2008, August). *The 2008 NIST Speaker Recognition Evaluation Results*. Accessed May 5, 2010 at http://www.itl.nist.gov/iad/mig/tests/sre/2008/official_results/index.html

Appendix C Glossary

This appendix provides definitions for security terminology used within or referenced in this document. The terms in the glossary are consistent with the terms used in the suite of FISMA-related security standards and guidelines developed by NIST. Unless otherwise stated, all terms used in this publication are also consistent with the definitions contained in the CNSS Instruction 4009, *National Information Assurance Glossary*.

Activities	An assessment object that includes specific protection related pursuits or actions supporting an information system that involve people (e.g., conducting system backup operations, monitoring network traffic).
Adequate Security [OMB Circular A130, Appendix III]	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost effective management, personnel, operational, and technical controls.
Advanced Persistent Threats	An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception), to generate opportunities to achieve its objectives, which are typically to establish and extend footholds within the information technology infrastructure of organizations for purposes of continually exfiltrating information, and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future. Moreover the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives.
Agency	See <i>Executive Agency</i>
Allocation	The process an organization employs to determine whether security controls are defined as system specific, hybrid, or common. The process an organization employs to assign security controls to specific information system components responsible for providing a particular security capability (e.g., router, server, remote sensor).
Application	A software program hosted by an information system.
Assessment	See <i>Security Control Assessment</i> .

Assessment Findings	Assessment results produced by the application of an assessment procedure to a security control or control enhancement to achieve an assessment objective; the execution of a determination statement within an assessment procedure by an assessor that results in either a <i>satisfied</i> or <i>other than satisfied</i> condition.
Assessment Method	One of three types of actions (i.e., examine, interview, test) taken by assessors in obtaining evidence during an assessment.
Assessment Object	The item (i.e., specifications, mechanisms, activities, individuals) upon which an assessment method is applied during an assessment.
Assessment Objective	A set of determination statements that expresses the desired outcome for the assessment of a security control or control enhancement.
Assessment Procedure	A set of assessment objectives and an associated set of assessment methods and assessment objects.
Assessor	See <i>Security Control Assessor</i> .
Assurance	The grounds for confidence that the set of intended security controls in an information system are effective in their application.
Assurance Case [Software Engineering Institute, Carnegie Mellon University]	A structured set of arguments and a body of evidence showing that an information system satisfies specific claims with respect to a given quality attribute.
Authentication [FIPS 200]	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See Authentication.
Authorization (to operate)	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed upon set of security controls.
Authorization Boundary [NIST SP 800-37]	All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is

	connected.
Authorize Processing	See <i>Authorization</i> .
Authorizing Official (AO) [NIST SP 800-37]	A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Authorizing Official Designated Representative [NIST SP 800-37]	An organizational official acting on behalf of an authorizing official in carrying out and coordinating the required activities associated with security authorization.
Availability [44 U.S.C., Sec. 3542]	Ensuring timely and reliable access to and use of information.
Basic Testing	A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. Also known as <i>Black Box Testing</i> .
Black Box Testing	See <i>Basic Testing</i> .
Categorization	The process of determining the security category (the restrictive label applied to classified or unclassified information to limit access) for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS 199 for other than national security systems.
Chief Information Officer (CIO) [PL 104-106, Sec. 5125(b)]	Agency official responsible for: 1) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; 2) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and 3) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.
Chief Information Security Officer	See Senior Agency Information Security Officer.
Common Control [NIST SP 800-37]	A security control that is inherited by one or more organizational information systems. See Security Control Inheritance.
Common Control Provider [NIST SP 800-37, Rev. 1]	An organizational official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information

	systems).
Compensating Security Controls [NIST SP 800-53]	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provide equivalent or comparable protection for an information system.
Comprehensive Testing	A test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. Also known as <i>White Box Testing</i> .
Computer Incident Response Team (CIRT)	Group of individuals usually consisting of Security Analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents. Also called a Computer Security Incident Response Team (CSIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability, or Cyber Incident Response Team).
Confidentiality [44 U.S.C., Sec. 3542]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Control (or Configuration Control) [CNSSI 4009]	Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.
Continuous Monitoring	Maintaining ongoing awareness to support organizational risk decisions. See <i>Information Security Continuous Monitoring, Risk Monitoring</i> and <i>Status Monitoring</i> .
Controlled Interface	A boundary with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information systems.
Controlled Unclassified Information	A categorical designation that refers to unclassified information that does not meet the standards for National Security classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the federal government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. Henceforth, the designation CUI replaces <i>Sensitive But Unclassified (SBU)</i> .
Countermeasures [CNSSI 4009]	Actions, devices, procedures, techniques, or other measures that

	reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
Cross Domain Solution	A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains.
Coverage	An attribute associated with an assessment method that addresses the scope or breadth of the assessment objects included in the assessment (e.g., types of objects to be assessed and the number of objects to be assessed by type). The values for the coverage attribute, hierarchically from less coverage to more coverage, are basic, focused, and comprehensive.
Data Loss	The exposure of proprietary, sensitive, or classified information through either data theft or data leakage.
Depth	An attribute associated with an assessment method that addresses the rigor and level of detail associated with the application of the method. The values for the depth attribute, hierarchically from less depth to more depth, are basic, focused, and comprehensive.
Domain [CNSSI 4009]	An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. See <i>Security Domain</i> .
Dynamic Subsystem	A subsystem that is not continually present during the execution phase of an information system. Service oriented architectures and cloud computing architectures are examples of architectures that employ dynamic subsystems.
Environment of Operation [NIST SP 800-37]	The physical surroundings in which an information system processes, stores, and transmits information.
Examine	A type of assessment method that is characterized by the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness over time.
Executive Agency [41 U.S.C., Sec. 403]	An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.
External Information System	An information system or component of an information system

(or Component)	that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
External Information System Service	An information system service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
External Information System Service Provider	A provider of external information system services to an organization through a variety of consumer producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain arrangements.
Federal Agency	See <i>Executive Agency</i> .
Federal Information System [40 U.S.C., Sec. 11331]	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
Federal Enterprise Architecture [FEA Program Management Office]	A business-based framework for government-wide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen centered, results-oriented, and market-based.
Focused Testing	A test methodology that assumes some knowledge of the internal structure and implementation detail of the assessment object. Also known as <i>Gray Box Testing</i> .
Gray Box Testing	See <i>Focused Testing</i> .
High-Impact System [FIPS 200]	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.
Hybrid Security Control [NIST SP 800-53]	A security control that is implemented in an information system in part as a common control and in part as a system-specific control. See <i>Common Control</i> and <i>System-Specific Security Control</i> .
Individuals	An assessment object that includes people applying specifications, mechanisms, or activities.

Industrial Control System	An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.
Information [FIPS 199]	An instance of an information type.
Information Owner [CNSSI 4009]	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information Resources [44 U.S.C., Sec. 3502]	Information and related resources, such as personnel, equipment, funds, and information technology.
Information Security [44 U.S.C., Sec. 3542]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Risk	The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and /or information systems.
Information Security Architect	Individual, group, or organization responsible for ensuring that the information security requirements necessary to protect the organization's core missions and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes.
Information Security Continuous Monitoring	Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.
Information Security Policy [CNSSI 4009]	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Information Security Program Plan [NIST SP 800-53]	Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.

Information Steward	Individual or group that helps to ensure the careful and responsible management of federal information belonging to the nation as a whole, regardless of the entity or source that may have originated, created, or compiled the information. Information stewards provide maximum access to federal information to elements of the federal government and its customers, balanced by the obligation to protect the information in accordance with the provisions of FISMA and any associated security- related federal policies, directives, regulations, standards, and guidance.
Information System [44 U.S.C., Sec. 3502]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Boundary	See <i>Authorization Boundary</i> .
Information System Owner (or Program Manager)	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Information System Security Engineer	Individual assigned responsibility for conducting information system security engineering activities.
Information System Security Engineering	Process that captures and refines information security requirements and ensures their integration into information technology component products and information systems through purposeful security design or configuration.
Information System related Security Risks	Information system-related security risks are those risks that arise through the loss of confidentiality, integrity, or availability of information or information systems and consider impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the nation. See <i>Risk</i> .
Information System Security Officer (ISSO) [CNSSI 4009]	Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program.
Information Technology [40 U.S.C., Sec. 1401]	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the

	use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term <i>information technology</i> includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Information Type [FIPS 199]	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.
Integrity [44 U.S.C., Sec. 3542]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Interview	A type of assessment method that is characterized by the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence, the results of which are used to support the determination of security control effectiveness over time.
Intrusion Detection and Prevention System (IDPS)	Software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.
Joint Authorization	Security authorization involving multiple authorizing officials.
Low-Impact System [FIPS 200]	An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.
Management Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
Measures	All the output produced by automated tools (e.g., IDS/IPS, vulnerability scanners, audit record management tools, configuration management tools, asset management tools) as well as various information security program-related data (e.g., training and awareness data, information system authorization data, contingency planning and testing data, incident response

	data). Measures also include security assessment evidence from both automated and manual collection methods.
Mechanisms	An assessment object that includes specific protection-related items (e.g., hardware, software, or firmware) employed within or at the boundary of an information system.
Metrics	Tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance- related data.
Moderate- Impact System [FIPS 200]	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate, and no security objective is assigned a FIPS 199 potential impact value of high.
National Security Information	Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.
National Security System [44 U.S.C., Sec. 3542]	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—(i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
Net-Centric Architecture	A complex system of systems composed of subsystems and services that are part of a continuously evolving, complex community of people, devices, information and services interconnected by a network that enhances information sharing and collaboration. Subsystems and services may or may not be developed or owned by the same entity, and, in general, will not be continually present during the full life cycle of the system of systems. Examples of this architecture include service- oriented

	architectures and cloud computing architectures.
Operational Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an Information system that are primarily implemented and executed by people (as opposed to systems).
Organization [FIPS 200, Adapted]	An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency, or, as appropriate, any of its operational elements).
Organizational Information Security Continuous Monitoring	Ongoing monitoring sufficient to ensure and assure effectiveness of security controls related to systems, networks, and cyberspace, by assessing security control implementation and organizational security status in accordance with organizational risk tolerance – and within a reporting structure designed to make real time, data driven risk management decisions.
Patch Management	The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.
Penetration Testing	A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.
Plan of Action & Milestones (POA&M) [OMB Memorandum 02-01]	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Potential Impact [FIPS 199]	The loss of confidentiality, integrity, or availability could be expected to have: (i) a <i>limited</i> adverse effect (FIPS 199 low); (ii) a <i>serious</i> adverse effect (FIPS 199 moderate); or (iii) a <i>severe</i> or <i>catastrophic</i> adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.
Reciprocity	Mutual agreement among participating organizations to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information.
Records	The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the

complete set of information on particular items).

Risk [FIPS 200, Adapted]

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.¹²

Risk Assessment

The process of identifying risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

**Risk Executive (Function)
[NIST SP 800-37]**

An individual or group within an organization that helps to ensure that: (i) security risk- related considerations for individual information systems, to include the authorization decisions, are viewed from an organization- wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and (ii) managing information system- related security risks is consistent across the organization, reflects organizational risk tolerance, and is considered along with organizational risks affecting mission/business success.

Risk Management

The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk- related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.

Risk Monitoring

Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions.

Risk Response

Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or

¹² Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation. Adverse impacts to the nation include, for example, compromises to information systems that support critical infrastructure applications or are paramount to government continuity of operations as defined by the Department of Homeland Security.


	reputation), organizational assets, individuals, other organizations, and the Nation.
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Safeguards [CNSSI 4009]	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with <i>Security Controls and Countermeasures</i> .
Security Authorization	See <i>Authorization</i> .
Security Categorization	The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS 199 for other than national security systems.
Security Controls [FIPS 199]	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Control Assessment	The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Security Control Assessor	The individual, group, or organization responsible for conducting a security control assessment.
Security Control Baseline [FIPS 200, Adapted]	One of the sets of minimum security controls defined for federal information systems in NIST Special Publication 800-53 and CNSS Instruction 1253.
Security Control Effectiveness	The measure of correctness of implementation (i.e., how consistently the control implementation complies with the security plan) and by how well the security plan meets organizational needs in accordance with current risk tolerance.
Security Control Enhancements	Statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control.
Security Control Inheritance	A situation in which an information system or application receives protection from security controls (or portions of security

	controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See <i>Common Control</i> .
Security Domain [CNSSI 4009]	A domain that implements a security policy and is administered by a single authority.
Security Impact Analysis	The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.
Security Management Dashboard [NIST SP 800-128]	A tool that consolidates and communicates information relevant to the organizational security posture in near-real time to security management stakeholders.
Security Objective [FIPS 199]	Confidentiality, integrity, or availability.
Security Plan	Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. See <i>System Security Plan</i> or <i>Information Security Program Plan</i> .
Security Policy [CNSSI 4009]	A set of criteria for the provision of security services.
Security Posture	The security status of an enterprise's networks, information, and systems based on IA resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes.
Security Requirements [FIPS 200]	Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
Senior (Agency) Information Security Officer (SISO) [44 U.S.C., Sec. 3544]	Official responsible for carrying out the Chief Information Officer responsibilities under the Federal Information Security Management Act (FISMA) and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. Note: Organizations subordinate to federal agencies may use the term <i>Senior Information Security Officer</i> or <i>Chief Information Security Officer</i> to denote individuals filling positions with similar responsibilities to Senior Agency Information Security Officers.

Senior Information Security Officer	See <i>Senior Agency Information Security Officer</i> .
Specification	An assessment object that includes document-based artifacts (e.g., policies, procedures, plans, system security requirements, functional specifications, and architectural designs) associated with an information system.
Status Monitoring	Monitoring the information security metrics defined by the organization in the information security continuous monitoring strategy.
Subsystem	A major subdivision of an information system consisting of information, information technology, and personnel that performs one or more specific functions.
Supplementation (Assessment Procedures)	The process of adding assessment procedures or assessment details to assessment procedures in order to adequately meet the organization's risk management needs.
Supplementation (Security Controls)	The process of adding security controls or control enhancements to a security control baseline from NIST Special Publication 800-53 or CNSS Instruction 1253 in order to adequately meet the organization's risk management needs.
System	See <i>Information System</i> .
System Security Plan [NIST SP 800-18]	Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
System-Specific Security Control [NIST SP 800-37]	A security control for an information system that has not been designated as a common security control or the portion of a hybrid control that is to be implemented within an information system.
System Development Life Cycle (SDLC)	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.
Tailored Security Control Baseline	A set of security controls resulting from the application of tailoring guidance to the security control baseline. See <i>Tailoring</i> .
Tailoring [NIST SP 800-53, CNSSI 4009]	The process by which a security control baseline is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization defined parameters in the security controls via explicit assignment and selection statements.

Tailoring (Assessment Procedures)	The process by which assessment procedures defined in Special Publication 800-53A are adjusted, or scoped, to match the characteristics of the information system under assessment, providing organizations with the flexibility needed to meet specific organizational requirements and to avoid overly constrained assessment approaches.
Technical Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
Test	A type of assessment method that is characterized by the process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior, the results of which are used to support the determination of security control effectiveness over time.
Threat [CNSSI 4009, Adapted]	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Threat Assessment [CNSSI 4009]	Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.
Threat Information	Information about types of attacks rather than specific threat actors.
Threat Source [FIPS 200]	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with Threat Agent.
Vulnerability [CNSSI 4009]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability Assessment [CNSSI 4009]	Formal description and evaluation of the vulnerabilities in an information system.
White Box Testing	See <i>Comprehensive Testing</i> .

Appendix A Security Requirements Traceability Matrix

 FVAP Security Requirement Traceability Matrix		Pilot Program Testing Requirements Security Gap Analysis		
		POC Name:	Michael Teribury (CALIBRE)	Jim Martin (CALIBRE)
		POC Phone:	(703) 588-8104	(703) 588-1179
		POC E-Mail:	michael.teribury.ctr@fvap.gov	James.Martin@calibresys.com
		Last Update: Jan. 31, 2011		
UOCAVA REQ. No. (1)	UOCAVA TEST REQ. (2)	TEST METHOD (3)	TEST ENTITY (4)	POTENTIAL IMPACT (5)
UOCAVA REQ. Number from "UOCAVA Pilot Program Test Requirements"	UOCAVA Req. from "UOCAVA Pilot Program Test Requirements"	UOCAVA Req. Test Method: Functional or Inspection	Test Entity: EAC, Manufacturer, or VSTL	<p>NIST SP800-30: The next major step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of a vulnerability.</p> <ul style="list-style-type: none"> • System mission (e.g., the processes performed by the IT system) • System and data criticality (e.g., the system's value or importance to an organization) • System and data sensitivity. <p>Rated on a Low, Medium or High Impact</p> <p>The following list provides a brief description of each security goal and the consequence (or impact) of its not being met:</p> <p>Loss of Integrity. System and data integrity refers to the requirement that information be protected from improper modification.</p> <p>Loss of Availability. If a mission-critical IT system is unavailable to its end users, the organization's mission may be affected.</p> <p>Loss of Confidentiality. System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data.</p>

LEGEND: TEST METHOD A=ANALYSIS D=DEMONSTRATION I=INSPECTION T=TEST		FVAP SRTM DEFINITIONS & EXPLANATIONS										
		VERIFICATION METHOD (6)		NIST Control No. (7)	IA Control Name (8)	ISO / IEC 17799 (9)	NIST SP800-26 (10)	GAO FISCAM (11)	DOD 8500.2 (12)	DCID 6/3 (13)	Related Control Guidance and References (14)	Mitigating IA Control (15)
The method for determining if the requirement that is being satisfactorily met. Includes Demonstration, Inspection or Test	NIST Special Publications IA Control Family	NIST Special Publications IA Control Family Name	International Standard Organization and International Electrotechnical Commission Reference Number	NIST SP800-26 Security Self-Assessment Guide Reference	Government Accounting Office Federal Information System Control Audit Manual	Depart of Defense 8500.1/2 IA guidance	Director of Central Intelligence Directive 6/3	Other federal, industry or international IA guidance applicable to this UOCAVA Pilot Program Testing Requirement	FVAP internal/external compensating control	See tab 3 CIA Triad	See tab 3 CIA Triad	

Gap Risk Analysis						
		Impact Rating			Compliant	
Availability	Mitigated	Low	Medium	High	Yes	No
See tab 3 CIA Triad	This UOCAVA Pilot Program Testing Requirement has been mitigated through another security control	See tab 3 CIA Triad	See tab 3 CIA Triad	See tab 3 CIA Triad	UOCAVA Pilot Program Testing Requirement meets guidance	UOCAVA Pilot Program Testing Requirement does NOT meet guidance
					None of the seven guidance documents has a direct reference to this UOCAVA test requirement	This is a UOCAVA test requirement that is functional and does not have a security related component
					No available reference	Functional Requirement



FVAP Security Requirement Traceability Matrix

FVAP Security Requirement Traceability Matrix		Pilot Program Testing Requirements Security Gap Analysis			LEGEND: TEST METHOD										Gap Risk Analysis												
					A=ANALYSIS																						
					D=DEMONSTRATION																						
					I=INSPECTION																						
		Last Update: Jan. 31, 2011			T=TEST																						
		FVAP SRTM DEFINITIONS & EXPLANATIONS																									
UOCAVA REQ. No. (1)	UOCAVA TEST REQ. (2)	TEST METHOD (3)	TEST ENTITY (4)	POTENTIAL IMPACT (5)	VERIFICATION METHOD (6)	NIST Control No. (7)	IA Control Name (8)	ISO / IEC 17799 (9)	NIST SP800-26 (10)	GAO FISCAM (11)	DOD 8500.2 (12)	DCID 6/3 (13)	Related Control Guidance and References (14)	Mitigating IA Control (15)	Confidentiality	Integrity	Availability	Mitigated	Low	Medium	High	Yes	No	No available reference	Functional Requirement	Reconciled in other documentation (Yes or No)	Identified Reference Documentation
4.3.1.2 Module testability	Each module SHALL have a specific function that can be tested and verified independently from the remainder of the code.	Inspection	Manufacturer	Relates to software integrity	I=INSPECTION	None	None	None	None	None	None	None	None	No reference documentation identified.	1					1				1	Yes	Found in Voting Systems Standards produced by the EAC. Other references relate to cryptographic modules within NIST Guidance and FIPS.	
4.3.1.3 Module size and identification	Modules SHALL be small and easily identifiable.	Inspection	Manufacturer	Relates to software integrity	I=INSPECTION	None	None	None	None	None	None	None	None	N/A	1					1			1	1	Yes	Good coding practices would dictate that modules be easily identified. The IEEE Software Engineering Body of Knowledge (SWEBOK) provides exception guidance and best practice knowledge that has been vetted by hundreds of industry experts. However, none of the additional reference documents speak to size of the modules.	
4.7.2.7 Nullify freed pointers	If pointers are used, any pointer variables that remain within scope after the memory they point to is deallocated SHALL be set to null or marked as invalid (pursuant to the idiom of the programming language used) after the memory they point to is deallocated.	Inspection	Manufacturer	Integrity and Availability; Relates to software quality and best programming practices. No specific security control.	I=INSPECTION	None	None	None	None	None	None	None	None	None	1	1			1				1		No	Good coding practices would dictate that all Null Pointers are reset. Additionally, there are specific requirements that agencies must follow when implementing cookies. See OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, available at: http://www.whitehouse.gov/omb/memoranda/m03-22.html.	
4.7.2.11 Election integrity monitoring	The voting system SHALL proactively detect or prevent basic violations of election integrity (e.g., stuffing of the ballot box or the accumulation of negative votes) and alert an election official or administrator if such violations they occur.	Inspection	Manufacturer	N/A to IT Security capability	I=INSPECTION	None	None	None	None	None	None	None	None Identified	N/A	1					1			1	1	Yes	A requirement of 4.1.4 of The Voting Over the Internet Pilot Project 2001.	
5.4.1.2 Cast vote integrity; storage	The integrity and authenticity of each individual cast vote SHALL be preserved by means of a digital signature during storage.	Functional	VSTL	Functional Requirement. Loss of Integrity.	T=TEST	None	None	None	None	None	None	None	Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006.	N/A	1					1	1		1		Yes	Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006.	
5.4.1.3 Cast vote storage	Cast vote data SHALL NOT be permanently stored on the vote capture device.	Functional	VSTL	Functional Requirement. Loss of Integrity.	T=TEST	None	None	None	None	None	None	None	Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006.	N/A	1					1			1	1	Yes	Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006.	
5.4.1.4 Electronic ballot box integrity	The integrity and authenticity of the electronic ballot box SHALL be protected by means of a digital signature.	Functional	VSTL	Functional Requirement. Loss of Integrity and/or Confidentiality.	T=TEST	None	None	None	None	None	None	None	Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006.	N/A	1					1			1	1	Yes	Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006.	
6.2 Components from Third Parties	A manufacturer who does not manufacture all the components of its voting system, but instead procures components as standard commercial items for assembly and integration into a voting system, SHALL verify that the supplier manufacturers follow documented quality assurance procedures that are at least as stringent as those used internally by the voting system manufacturer.	Inspection	Manufacturer	loss of Integrity, availability and/or Confidentiality	I=INSPECTION	None	None	None	None	None	None	None	Nothing found in referenced documentation. However, this may be referenced within another publication involving acquisitions.	N/A	1	1	1			1				1		Yes	The June 2010 Accessibility and Usability Consideration of Remote Voting Systems DRAFT Whitepaper prepared by NIST discusses 3rd party components. It specifically recommends that "design and test voting system components against standards and guidelines for interoperability and test all likely configurations."
6.3 Responsibility for Tests	Manufacturer SHALL be responsible for performing all quality assurance tests, acquiring and documenting test data, and providing test reports for examination by the VSTL as part of the national certification process. These reports SHALL also be provided to the purchaser upon request.	Inspection	Manufacturer	loss of Integrity or availability	I=INSPECTION	None	None	None	None	None	None	None	Nothing found in referenced documentation. However, this may be referenced within another publication involving acquisitions.	N/A	1	1				1				1		No	No reference materials define responsibility for manufacturer to test systems.
7.5.2 Functional Configuration Audit (FCA)	The Functional Configuration Audit is conducted by the VSTL to verify that the voting system performs all the functions described in the system documentation. Manufacturers SHALL: a. Completely describe its procedures and related conventions used to support this audit for all voting system components; and b. Provide the following information to support this audit: c. Copies of all procedures used for module or unit testing, integration testing, and system testing; d. Copies of all test cases generated for each module and integration test, and sample ballot formats or other test cases used for system tests; and e. Records of all tests performed by the procedures listed above, including error corrections and retests.	Functional / Inspection	VSTL	Configuration/Testing	I=INSPECTION	None	None	None	None	None	None	None	N/A	N/A	1	1	1			1				1		Yes	Technical Guidelines Development Committee to the Election Assistance Commission: A reference was located in Chapter 4: Documentation and Design Reviews (Inspection) under section 4.1-A Applies to Voting Systems: An accredited test lab SHALL verify that the documentation submitted by the manufacturer in the TDP meets all the requirements applicable to the TDP, is sufficient to enable the inspections specified in this chapter, and is sufficient to enable tests specified.
8.2.1 TDP Implementation Statement	The TDP SHALL include an implementation statement.	Inspection	Manufacturer	Documentation	I=INSPECTION	None	None	None	None	None	None	None	None	N/A		1			1					1	1	Yes	This requirement is only mentioned in the VVSG Recommendations to the EAC in Chapter 2-10.
8.3.4.1 Hardwired and mechanical implementations of logic	For each non-COTS hardware component (e.g., an application-specific integrated circuit or a manufacturer-specific integration of smaller components), manufacturers SHALL provide complete design and logic specifications, such as Computer Aided Design and Hardware Description Language files.	Inspection	Manufacturer	Industrial control logic could impact Confidentiality, Integrity and/or Availability.	I=INSPECTION	None	None	None	None	None	None	None	NIST SP800-53 Reference: An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.	Full Documentation of boarder logic and identification of all devices. Border logic should be minimized.	1	1	1				1			1		No	This falls under "border Logic" within the definition found in Appendix A of VVSG-0807. This does represent a significant threat to integrity and confidentiality.

8.3.4.2 Logic specifications for PLDs, FPGAs and PICs	For each Programmable Logic Device (PLD), Field-Programmable Gate Array (FPGA), or Peripheral Interface Controller (PIC) that is programmed with non-COTS logic, manufacturers SHALL provide complete logic specifications, such as Hardware Description Language files or source code.	Inspection	Manufacturer	Industrial control logic could impact Confidentiality, Integrity and/or Availability.	I=INSPECTION	None	None	None	None	None	None	None	NIST SP800-53 Reference: An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.	Full Documentation of boarder logic and identification of all devices. Border logic should be minimized.	1	1	1					1								1		No	This falls under "border Logic" within the definition found in Appendix A of VVSG-0807. This does represent a significant threat to integrity and confidentiality.
8.4.5.3 Justify coding conventions	Manufacturers SHALL furnish evidence that the selected coding conventions are "published" and "credible" as specified in section 4.3.1.	Inspection	Manufacturer	Documentation normally contained within the System Security Plan under "robustness". Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	None	None	None	None	None	None	None	non-proprietary References coding practices. OCID 603.1.H.1 in the following pages, the term "good engineering practice" refers to the state of the engineering art for commercial systems that have equivalent problems and solutions; a good engineering practice by definition meets commercial requirements. These practices are usually part of the normal installation and operating procedures for systems. When placing security reliance on items that implement good engineering practice (such as commercial off-the shelf (COTS) software), the DAAs or their designees shall verify that the item(s) are set up properly and are accessible.	Full Documentation of boarder logic and identification of all devices, manufacturer and design.	1	1	1					1								1		No	There is a discussion DRAFT posted on Dec. 1, 2006 regarding coding convention and logic verification that was prepared by NIST for the TGDC. This paper outlines specific requirements and guidance for coding best practices.
8.4.6.1 Application logic operating environment	Manufacturers SHALL describe or make reference to all operating environment factors that influence the design of application logic.	Inspection	Manufacturer	Documentation normally contained within the System Security Plan under "robustness". Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	None	None	None	None	None	None	None	PE-1 through PE-19 define environmental controls and related requirements.		1	1	1					1							1		Yes	NIST SP800-18 provides guidance for operating environments.	
8.4.7.1 Hardware environment and constraints	Manufacturers SHALL identify and describe the hardware characteristics that influence the design of the application logic, such as: a. Logic and arithmetic capability of the processor; b. Memory read-write characteristics; c. External memory device characteristics; d. Peripheral device interface hardware; e. Data input/output device protocols; and f. Operator controls, indicators, and displays.	Inspection	Manufacturer	Documentation normally contained within the System Security Plan under "robustness". Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	None	None	None	None	None	None	None	PE-1 through PE-19 define environmental controls and related requirements.		1	1	1					1							1		Yes	NIST SP800-18 provides guidance for operating environments.	
8.4.8.2 Compilers and assemblers	For systems containing compiled or assembled application logic, manufacturers SHALL identify the COTS compilers or assemblers used in the generation of executable code, and the specific versions thereof.	Inspection	Manufacturer	Documentation normally contained within the System Security Plan. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	None	None	None	None	None	None	None. Only references backups should provide for the protection of compilers.	None. Only references backups should provide for the protection of compilers.		1	1	1					1							1		Yes	The TGDC Recommendations from August, 2007 specify requirements. There are numerous IEEE standards and requirements defined that relate to compilers and assemblers.	
8.4.8.3 Interpreters	For systems containing interpreted application logic, manufacturers SHALL specify the COTS runtime interpreter that SHALL be used to run this code, and the specific version thereof.	Inspection	Manufacturer	Documentation normally contained within the System Security Plan. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	None	None	None	None	None	None	None. Only references backups should provide for the protection of compilers.	None. Only references backups should provide for the protection of compilers.		1	1	1					1							1		No	No specific NIST or IEEE requirement located.	
8.4.9.1 Application logic functional specification	Manufacturers SHALL provide a description of the operating modes of the system and of application logic capabilities to perform specific functions.	Inspection	Manufacturer	Documentation normally contained within the System Security Plan. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTION	None	None	None	None	None	None	None	None		1	1	1					1							1		No	No specific NIST or IEEE requirement located.	
9.2.3.3 Traceability of procured software	The system description SHALL include a declaration that procured software items were obtained directly from the manufacturer or from a licensed dealer or distributor.	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTION	None	None	None	None	None	None	None			1	1	1					1							1		Yes	The DOE has a specific requirement for traceability of procured software.	
9.4.5.1 Ballot count and vote total auditing	The system's user documentation SHALL fully specify a secure, transparent, workable and accurate process for producing all records necessary to verify the accuracy of the electronic tabulation result.	Inspection	Manufacturer	Loss of data Integrity	I=INSPECTION	None	None	None	None	None	None	None	None		1	1	1					1							1		Yes	IEEE P1583 speaks to voting system standards for election accuracy, and auditable results.	
9.5.1.4 Election specific software identification	Manufacturers SHALL identify election specific software in the user documentation.	Inspection	Manufacturer	No security impact	I=INSPECTION	None	None	None	None	None	None	None	Special denotation within the supplied documentation			1					1								1		No	This requirement is not clear as to its meaning. Now references available. However, this is a good security practice and should be followed.	
9.5.1.7 Compiler installation prohibited	The software installation procedures used to install software on programmed devices of the system SHALL specify that no compilers SHALL be installed on the programmed device.	Inspection	Manufacturer	No direct security implication of this addition to the documentation. However, installation of compilers could impact confidentiality, availability and integrity.	I=INSPECTION	None	None	None	None	None	None	End user software is prohibited. However, no specific guidance on compilers within the referenced documentation.	None		1	1	1					1							1		No	Now references available. However, this is a good security practice and should be followed.	
9.6.1.2 Setup inspection record generation	The setup inspection process SHALL describe the records that result from performing the setup inspection process.	Inspection	Manufacturer	This requirement could impact Confidentiality and/or integrity and availability.	I=INSPECTION	None	None	None	None	None	None	None	NIST SP800-100 States: In addition, developing a security requirements checklist based on the security requirements specified for the system during the conceptual, design, and implementation phases of the SDLC can be used to provide a 360-degree inspection of the system.	None		1	1	1					1					1		No	No specific reference documentation for this requirement.		
9.6.1.12 Consumables quantity of vote capture device	Manufacturers SHALL provide a list of consumables associated with the vote capture device, including estimated number of usages per quantity of consumable.	Inspection	Manufacturer	No known security risk.	I=INSPECTION	None	None	None	None	None	None	No specific IA Control referenced.	None			1													1		No	This is specific to the voting system. NIST H143 makes a brief reference to consumables. However, this is a reasonable requirement. Media storage is a requirement of NIST guidance for DIACAP, and while it is not specifically mentioned, it would be reasonable to assume that it would fall under this guidance.	
9.6.1.13 Consumable inspection procedure	Manufacturers SHALL provide the procedures to inspect the remaining amount of each consumable of the vote capture device.	Inspection	Manufacturer	No known security risk.	I=INSPECTION	None	None	None	None	None	None	No specific IA Control referenced.	None			1													1		No	This is specific to the voting system. NIST H143 makes a brief reference to consumables. However, this is a reasonable requirement. Media storage is a requirement of NIST guidance for DIACAP, and while it is not specifically mentioned, it would be reasonable to assume that it would fall under this guidance.	
9.6.1.14 Calibration of vote capture device components nominal range	Manufacturers SHALL provide a list of components associated with the vote capture devices that require calibration and the nominal operating ranges for each component.	Inspection	Manufacturer	No known security risk.	I=INSPECTION	None	None	None	None	None	None	No specific IA Control referenced.	None			1													1		No	This should fall under the SSP guidance. However, this is election specific, and no other reference documentation was located.	
9.6.1.15 Calibration of vote capture device components inspection procedure	Manufacturers SHALL provide the procedures to inspect the calibration of each component.	Inspection	Manufacturer	No known security risk.	I=INSPECTION	None	None	None	None	None	None	No specific IA Control referenced.	None			1													1		Yes	This is a HAVA requirement under Quality Assurance and Configuration Management.	



FVAP Security Requirement Traceability Matrix

FVAP Security Requirement Traceability Matrix		UOCAVA Pilot Program Testing Requirements Security Gap Analysis			LEGEND: TEST METH A=ANALYSIS D=DEMONSTRATION I=INSPECTION T=TEST												Gap Risk Analysis											
		POC Name:															Risk			Impact Rating			Compliant			Recommended Technical or UOCAVA Requirement Change N/C = No Change		
		POC Phone:															Confidentiality	Integrity	Availability	Mitigated	Low	Medium	High	Yes	No		No available reference	Functional Requirement
		POC E-Mail:																										
		Last Update: Jan.31, 2011																										
UOCAVA REQ. No. (1)	UOCAVA TEST REQ. (2)	TEST METHOD (3)	TEST ENTITY (4)	POTENTIAL IMPACT (5)	VERIFICATION METHOD (6)	NIST Control No. (7)	IA Control Name (8)	ISO / IEC 17799 (9)	NIST SP800-26 (10)	GAO FISCAM (11)	DOD 8500.2 (12)	DCID 6/3 (13)	Related Control Guidance and References (14)	Mitagating IA Control (15)														
2.1.1.1 Component accuracy	Memory hardware, such as semiconductor devices and magnetic storage media, SHALL be accurate.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST & Demonstration	MP-1	Media Protection Policy and Procedures	10.1.1 10.7 15.1.1 15.1.3	8.2	---	PESP-1 DCAR-1	DCID: B.2.a Manual: 2.B.6.c(7) 8.B.2		N/A	1	1	1					1	1				N/C	
2.1.1.2 Equipment design	The design of equipment in all voting systems SHALL provide for protection against mechanical, thermal, and electromagnetic stresses that impact voting system accuracy.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST & Demonstration	MP-2	Media Access	10.7.3	8.2.1; 8.2.2; 8.2.3; 8.2.6; 8.2.7	---	PEDI-1; PEPF-1	2.B.9.b(4); 4.B.1.a(1); 4.B.1.a(7)		N/A	1	1	1					1	1				N/C	
2.1.1.3 Voting system accuracy	To ensure vote accuracy, all voting systems SHALL: a. Record the election contests, candidates, and issues exactly as defined by election officials; b. Record the appropriate options for casting and recording votes; c. Record each vote precisely as indicated by the voter and be able to produce an accurate report of all votes cast; d. Include control logic and data processing methods incorporating parity and check-sums (or equivalent error detection and correction methods) to demonstrate that the voting system has been designed for accuracy; and e. Provide software that monitors the overall quality of data read-write and transfer quality status, checking the number and types of errors that occur in any of the relevant operations on data and how they were corrected.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST & Demonstration	SI-10	Information Accuracy, Completeness, Validity, and Authenticity	10.7.3; 12.2.1; 12.2.2	---	---	---	7.B.2.h; 2.B.4.d		N/A	1	1	1					1	1				N/C	
2.1.2 Environmental Range	All voting systems SHALL meet the accuracy requirements over manufacturer specified operating conditions and after storage under non-operating conditions.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST & Demonstration	None	None	None	None	None	None	None	FIPS 200; NIST Special Publications 800-12, 800-14, 800-66, 800-100. Protecting information residing on portable and mobile devices (e.g., employing cryptographic mechanisms to provide confidentiality and integrity protections during storage and while in transit when outside of controlled areas) is covered in the media protection family. Related security controls: MP-4, MP-5.	The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.	1	1	1					1				1	N/C	
2.1.3.1 Election management system accuracy	Voting systems SHALL accurately record all election management data entered by the user, including election officials or their designees.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST & Demonstration	PL-3	System Security Plan Update	6.1	3.2.10; 5.2.1	SP-2.1	5.7.5	2.B.7.c(5)		Significant changes are defined in advance by the organization and identified in the configuration management process. NIST Special Publication 800-18 provides guidance on security plan updates.	1	1	1					1	1				N/C	
2.1.3.2 Recording accuracy	For recording accuracy, all voting systems SHALL: a. Record every entry made by the user except where it violates voter privacy; b. Accurately interpret voter selection(s) and record them correctly to memory; c. Verify the correctness of detection of the user selections and the addition of the selections correctly to memory; d. Verify the correctness of detection of data entered directly by the user and the addition of the selections correctly to memory; and e. Preserve the integrity of election management data stored in memory against corruption by stray electromagnetic emissions, and internally generated spurious electrical signals.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST & Demonstration	SI-10	Information Accuracy, Completeness, Validity, and Authenticity	10.7.3; 12.2.1; 12.2.2	---	---	---	7.B.2.h; 2.B.4.d		N/A	1	1	1					1	1				N/C	
2.1.4 Telecommunications Accuracy	The telecommunications components of all voting systems SHALL achieve a target error rate of no more than one in 10,000,000 ballot positions, with a maximum acceptable error rate in the test process of one in 500,000 ballot positions.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST & Demonstration	None	None	None	None	None	None	None			1	1	1					1	1				N/C	
2.1.5.1 Simulators	If a simulator is used, it SHALL be verified independently of the voting system in order to produce ballots as specified for the accuracy testing.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted. Inaccurate testing with potential false validation of results.	A=ANALYSIS	None	None	None	None	None	None	None			1	1	1					1				1	N/C	
2.1.5.2 Ballots	Ballots used for accuracy testing SHALL include all the supported types (i.e., rotation, alternative languages) of contests and election types (primary, general).	Functional	VSTL	Functional requirement with no direct security impact.	T=TEST & Demonstration	None	None	None	None	None	None	None				1					1					1	N/C	

2.1.6 Reporting Accuracy	Processing accuracy is defined as the ability of the voting system to process stored voting data. Processing includes all operations to consolidate voting data after the voting period has ended. The voting systems SHALL produce reports that are consistent, with no discrepancy among reports of voting data.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST & Demonstration	SI-7	Software and Information Integrity	12.2.1; 12.2.2; 12.2.4	11.2.1; 11.2.4	---	FVAP UOCA ECSD-2	4.B.1.c(2); 5.B.1.a(3); 5.B.2.a(6)	ECAT-2 Audit Trail, Monitoring, Analysis and Reporting; ECTP-1 Audit Trail Protection SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY	N/A		1									1	1						4/2/20	N/C
2.2.1 Maximum Capacities	The manufacturer SHALL specify at least the following maximum operating capacities for the voting system (i.e. server, vote capture device, tabulation device, and communications links): Throughput, Memory, Transaction processing speed, and Election constraints: Number of jurisdictions Number of ballot styles per jurisdiction Number of contests per ballot style Number of candidates per contest Number of voted ballots	Functional	VSTL	No direct security impact	T=TEST & Demonstration	None	None	None	None	None	None	None		N/A					1										1		N/C		
2.2.1.1 Capacity testing	The voting system SHALL achieve the maximum operating capacities stated by the manufacturer in section 2.2.1.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST & Demonstration	None	None	None	None	None	None	None			1	1	1								1					1		N/C	
2.2.2 Operating Capacity notification	The voting system SHALL provide notice when any operating capacity is approaching its limit.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST & Demonstration	None	None	None	None	None	None	None			1	1	1								1					1		N/C	
2.2.3 Simultaneous Transmissions	The voting system SHALL protect against the loss of votes due to simultaneous transmissions.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST & Demonstration	SC-8	Transmission Integrity	10.6.1; 10.8.1; 10.9.1	11.2.1; 11.2.4; 11.2.9; 16.2.14	AC-3.2	ECTM-1 Transmission Integrity Controls ECTM-2 Transmission Integrity Controls	5.B.3.a(11)	NIST Special Publication 800-52 provides guidance on protecting transmission integrity using Transport Layer Security (TLS). NIST Special Publication 800-77 provides guidance on protecting transmission integrity using IPsec. NIST Special Publication 800-81 provides guidance on Domain Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems. Others include: FIPS 198; NIST Special Publications 800-44, 800-45, 800-49, 800-52, 800-57, 800-54, 800-58, 800-66, 800-77, 800-81, 800-95, 800-97	N/A		1									1	1					N/C		
2.3.1.1 Import the election definition	The voting system SHALL: a. Keep all data logically separated by, and accessible only to, the appropriate state and local jurisdictions; b. Provide the capability to import or manually enter ballot content, ballot instructions and election rules, including all required alternative language translations from each jurisdiction; c. Provide the capability for the each jurisdiction to verify that their election definition was imported accurately and completely; d. Support image files (e.g., jpg or gif) and/or a handwritten signature image on the ballot so that state seals, official signatures and other graphical ballot elements may be properly displayed; and e. Support multiple ballot styles per each local jurisdiction.	Inspection / Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST & Demonstration	PE-2 AC-5 SEPARATION OF DUTIES	Physical Access Authorizations	9.1.2; 9.1.6; 10.1.3; 10.6.1; 10.10.1	7.1.1; 7.1.2; 6.1.1; 6.1.2; 6.1.3; 15.2.1; 16.1.2; 17.1.5	AC-3.1; AC-3.2; SD-1.2	PECF-1 DCPA-1 Partitioning the Application ECCD-2 Changes to Data PRAS-2 Access to Information ECLP-1	4.B.1.a(1); 8.E; 2.A.1; 4.B.3.a(18)	The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.	Discretionary Access Control (DAC). A means of restricting access to an object (e.g., files, data entities) based on the identity and need-to-know of a subject (e.g., user, process) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) to any other subject (unless restrained by a mandatory access control).	1	1	1				1					1	1					Graphic formats are subject to corruption and remote code execution when malformed. Graphic file formats should be evaluated for potential risks and vulnerabilities. Appropriate Microsoft security bulletins and patches should be updated prior to elections.	
2.3.1.2 Protect the election definition	The voting system SHALL provide a method to protect the election definition from unauthorized modification.	Functional	VSTL	A loss of integrity is the unauthorized modification or destruction of information. Information, the loss, misuse, or unauthorized access to or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of title 5, United States Code,	T=TEST & Demonstration	SI-7	Software and Information Integrity	12.2.1; 12.2.2; 12.2.4	11.2.1; 11.2.4	---	ECSD-2	4.B.1.c(2); 5.B.1.a(3); 5.B.2.a(6)		Information Security [44 U.S.C., Sec. 3542] The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Integrity [44 U.S.C., Sec. 3542] Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	1	1									1	1					Does not specify how this is to be accomplished. No recommendation		
2.3.2.1 Voting system test mode	The voting system SHALL provide a test mode to verify that the voting system is correctly installed, properly configured, and all functions are operating to support pre-election readiness testing for each jurisdiction.	Functional	VSTL	A system self test. NIST has SP800-126 Rev. 1 DRAFT Technical Specifications for the Security Content Automation Protocol (SCAP) that may relate testing requirements and specifications for security software flaws.	T=TEST & Demonstration	None	None	None	None	None	None	None		No specific findings for diagnostics or test mode analysis. However, remote diagnostic is mentioned.	1	1	1								1					1		N/C	
2.3.2.2 Test data segregation	The voting system SHALL provide the capability to zero-out or otherwise segregate test data from actual voting data.	Functional	VSTL	Functional test.	T=TEST & Demonstration	None	None	None	None	None	None	None			1	1	1						1						1		N/C		
2.4.1.1 Accessing the ballot	The voting system SHALL: a. Present the correct ballot style to each voter; b. Allow the voting session to be canceled; and c. Prevent a voter from casting more than one ballot in the same election.	Functional	VSTL	Functional test.	T=TEST & Demonstration	None	None	None	None	None	None	None			1	1	1								1					1		N/C	

2.4.2.1 Record voter selections	The voting system SHALL: a. Record the selection and non-selection of individual vote choices; b. Record the voter's selection of candidates whose names do not appear on the ballot, if permitted under state law, and record as many write-ins as the number of candidates the voter is allowed to select; c. Prohibit the voter from accessing or viewing any information on the display screen that has not been authorized and preprogrammed into the voting system (i.e., no potential for display of external information or linking to other information sources); d. Allow the voter to change a vote within a contest before advancing to the next contest; e. Provide unambiguous feedback regarding the voter's selection, such as displaying a checkmark beside the selected option or conspicuously changing its appearance; f. Indicate to the voter when no selection, or an insufficient number of selections, has been made for a contest (e.g., undervotes); g. Provide the voter the opportunity to correct the ballot for an undervote before the ballot is cast; h. Allow the voter, at the voter's choice, to submit an undervoted ballot without correction. i. Prevent the voter from making more than the allowable number of selections for any contest (e.g., overvotes); and j. In the event of a failure of the main power supply external to the voting system, provide the capability for any voter who is voting at the time to complete casting a ballot, allow for the successful shutdown of the voting system without loss or degradation of the voting and audit data, and allow voters to resume voting once the voting system has reverted to back-up power.	Functional	VSTL	Functional test.	D=DEMONSTRATION	None	None	None	None	None	None	None			1	1	1								1			1	N/C	4/2/2015				
2.4.2.2 Verify voter selections	The voting system SHALL: a. Produce a paper record each time the confirmation screen is displayed; b. Generate a paper record identifier. This SHALL be a random identifier that uniquely links the paper record with the cast vote record; c. Allow the voter to either cast the ballot or return to the vote selection process to make changes after reviewing the confirmation screen and paper record; and d. Prompt the voter to confirm his choices before casting the ballot, signifying to the voter that casting the ballot is irrevocable and directing the voter to confirm his intention to cast the ballot.	Functional	VSTL	Functional test.	D=DEMONSTRATION	None	None	None	None	None	None	None			1	1	1								1			1	N/C					
2.4.2.3 Cast ballot	The voting system SHALL: a. Store all cast ballots in a random order; logically separated by, and only accessible to, the appropriate state/local jurisdictions; b. Notify the voter after the vote has been stored persistently that the ballot has been cast; c. Notify the voter that the ballot has not been cast successfully if it is not stored successfully, and provide clear instruction as to steps the voter should take to cast his ballot should this event occur; and d. Prohibit access to voted ballots until such time as state law allows for processing of absentee ballots.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	PE-2 AC-5 SEPARATION OF DUTIES	Physical Access Authorizations	9.1.2; 9.1.6; 10.1.3; 10.6.1; 10.10.1	7.1.1; 7.1.2; 6.1.1; 6.1.2; 6.1.3; 15.2.1; 16.1.2; 17.1.5	AC-3.1; AC-3.2; SD-1.2	PECF-1 DCPA-1 Partitioning the Application ECCD-2 Changes to Data PRAS-2 Access to Information ECLP-1	4.B.1.a(1); 8.E; 2.A.1; 4.B.3.a(18)	The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.	Discretionary Access Control (DAC). A means of restricting access to an object (e.g., files, data entities) based on the identity and need-to-know of a subject (e.g., user, process) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) to any other subject (unless restrained by a mandatory access control).	1	1	1							1	1						N/C			
2.4.2.4.1 Absentee model	The cast ballot SHALL be linked to the voter's identity without violating the privacy of the voter.	Functional	VSTL	Privacy requirements and Audit Trail Requirements	D=DEMONSTRATION	None	None	None	None	None	None	None		National Institute of Standards and Technology Federal Information Processing Standards Publication 201-1, Personal Identity Verification of Federal Employees and Contractors, March 2006.	1	1								1				1	N/C					
2.4.2.4.2 Early voting model	The cast ballot SHALL NOT be linked to the voter's identity.	Inspection	VSTL	Privacy requirements and Audit Trail Requirements	D=DEMONSTRATION	None	None	None	None	None	None	None			1									1				1	N/C					
2.4.3.1 Link to voter	The voting system SHALL be capable of producing a cast vote record that does not contain any information that would link the record to the voter.	Functional	VSTL	Integrity: Privacy requirements and Audit Trail Requirements	D=DEMONSTRATION	None	None	None	None	None	None	None			1									1				1	N/C					
2.4.3.2 Voting session records	The voting system SHALL NOT store any information related to the actions performed by the voter during the voting session.	Functional	VSTL	Integrity: Privacy requirements and Audit Trail Requirements	T=TEST & Demonstration	None	None	None	None	None	None	None			1	1								1				1	N/C					
2.5.1.1 Seal and sign the electronic ballot box	The voting system SHALL seal and sign each jurisdiction's electronic ballot box, by means of a digital signature, to protect the integrity of its contents.	Functional	VSTL	Integrity: Privacy requirements and Audit Trail Requirements	T=TEST & Demonstration	None	None	None	None	None	None	None	NIST FIPS 140-2 validated cryptography (e.g., DoD PKI class 3 or 4 token) is used to implement encryption (e.g., AES, 3DES, DES, Skipjack), key exchange (e.g., FIPS 171), digital signature (e.g., DSA, RSA, ECDSA), and hash (e.g., SHA-1, SHA-256, SHA-384, SHA-512). Newer standards should be applied as they become available.	National Institute of Standards and Technology Federal Information Processing Standards Publication 186-2, Digital Signature Standard (DSS), January 2000. National Institute of Standards and Technology Federal Information Processing Standards Publication 186-3 (Draft), Digital Signature Standard (DSS), March 2006. National Institute of Standards and Technology Special Publication 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications November 2006.			1								1						1	N/C		
2.5.1.2 Electronic ballot box retrieval	The voting system SHALL allow each jurisdiction to retrieve its electronic ballot box.	Functional	VSTL	Functional Requirement	T=TEST & Demonstration	None	None	None	None	None	None	None			1	1	1							1				1	N/C					
2.5.1.3 Electronic ballot box integrity check	The voting system SHALL perform an integrity check on the electronic ballot box verifying that it has not been tampered with or modified before opening.	Functional	VSTL	Functional Requirement	T=TEST & Demonstration	None	Physical Access Control	None	None	None	None	None			1	1	1							1				1	N/C					
2.5.2.1 Tabulation device connectivity	The tabulation device SHALL be physically, electrically, and electromagnetically isolated from any other computer network.	Inspection	VSTL	Functional Requirement related to a loss of integrity	T=TEST & Demonstration	None	None	None	None	None	DCSP-1 EBBD-2	None	DCSP-1 Security Support Structure Partitioning: The security support structure is isolated by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform security functions. The security support structure maintains separate execution domains (e.g., address spaces) for each executing process. EBBD-2 Boundary Defense Boundary: defense mechanisms to include firewalls and network intrusion detection systems (IDS) are deployed at the enclave boundary to the wide area network, at layered or internal enclave boundaries and at key points in the network, as required. All Internet access is proxied through Internet access points that are under the management and control of the enclave and are isolated from other DoD information systems by physical or logical means.	Control: The organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility. The organization controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.	1	1	1						1					1				1	N/C	

2.5.2.2 Open ballot box	The tabulation device SHALL allow only an authorized entity to open the ballot box.	Functional	VSTL	Functional Requirement related to a loss of confidentiality due to physical access	T=TEST & Demonstration	PE-1 PE-2 PE-3 PE-6	Physical and Environmental Protection Policy and Procedures	15.1.1	7	PETN-1; DCAR-1	DCID: B.2.a; Manual: 2.B.4.e(5)	8.D	PECF-2 Access to Computing Facilities Only authorized personnel with appropriate clearances are granted physical access to computing facilities that process classified information.PECF-1 Access to Computing Facilities Only authorized personnel with a need-to-know are granted physical access to computing facilities that process sensitive information or unclassified information that has not been cleared for release. PEPF-1 Physical Protection of Facilities Every physical access point to facilities housing workstations that process or display sensitive information or unclassified information that has not been cleared for release is controlled during working hours and guarded or locked during non-work hours.	Control: The organization develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and issues appropriate authorization credentials. Designated officials within the organization review and approve the access list and authorization credentials [Assignment: organization-defined frequency, at least annually].	1	1	1						1	1									4/2/2015 N/C				
2.5.2.3.1 Adjudication	The tabulation device SHALL allow the designation of electronic ballots as "accepted" or "not accepted" by an authorized entity.	Functional	VSTL	Functional Requirement related to Operations and Integrity. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None					1								1						1	N/C					
2.5.2.4 Ballot decryption	The tabulation device decryption process SHALL remove all layers of encryption and breaking all correlation between the voter and the ballot, producing a record that is in clear text.	Functional	VSTL	Functional Requirement related to Operations and Confidentiality. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None					1	1							1						1	N/C					
2.5.2.5 Tabulation report format	The tabulation device SHALL have the capability to generate a tabulation report of voting results in an open and non-proprietary format.	Functional	VSTL	Functional Requirement related to Operations. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None					1	1							1						1	N/C					
2.6.2.1 All records capable of being exported	The voting system SHALL provide the capability to export its electronic records in an open format, such as XML, or include a utility to export log data into a publicly documented format.	Functional	VSTL	Functional Requirement related to Operations. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None					1	1					1								1	N/C					
2.6.2.2 Ballot images	The voting system SHALL have the capability to generate ballot images in a human readable format.	Functional	VSTL	Functional Requirement related to Operations. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None					1						1								1	Ballot Image format should meet security requirements in 2.3.1.1					
2.6.2.3 Ballot image content	The voting system SHALL be capable of producing a ballot image that includes: a. Election title and date of election; b. Jurisdiction identifier; c. Ballot style; d. Paper record identifier; and e. For each contest and ballot question: i. The choice recorded, including write-ins; and ii. Information about each write-in.	Functional	VSTL	Functional Requirement related to Operations. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None					1	1							1						1	Ballot Image format should meet security requirements in 2.3.1.1					
2.6.2.4 All records capable of being printed	The tabulation device SHALL provide the ability to produce printed forms of its electronic records. The printed forms SHALL retain all required information as specified for each record type other than digital signatures.	Functional	VSTL	Functional Requirement related to Operations. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None					1	1							1						1	N/C					
2.6.2.5 Summary count record	The voting system SHALL produce a summary count record including the following: a. Time and date of summary record; and b. The following, both in total and broken down by ballot style and voting location: i. Number of received ballots ii. Number of counted ballots iii. Number of rejected electronic CVRs iv. Number of write-in votes v. Number of undervotes.	Functional	VSTL	Functional Requirement related to Operations. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None	None Identified	N/A				1						1							1	N/C					
2.6.3.1 Paper record creation	Each vote capture device SHALL print a human readable paper record.	Functional	VSTL	Functional Requirement related to Operations. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None	None Identified	N/A				1						1							1	N/C					
2.6.3.2 Paper record contents	Each paper record SHALL contain at least: a. Election title and date of election; b. Voting location; c. Jurisdiction identifier; d. Ballot style; e. Paper record identifier; and f. For each contest and ballot question: i. The recorded choice, including write-ins; and ii. Information about each write-in.	Inspection	VSTL	Functional Requirement related to Operations. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None	None Identified	N/A				1						1							1	N/C					
2.6.3.3 Privacy	The vote capture device SHALL be capable of producing a paper record that does not contain any information that could link the record to the voter.	Inspection	VSTL	Functional Requirement related to Operations and Confidentiality. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None	None Identified	N/A			1	1							1							1	N/C				
2.6.3.4 Multiple pages	When a single paper record spans multiple pages, each page SHALL include the voting location, ballot style, date of election, and page number and total number of the pages (e.g., page 1 of 4).	Functional	VSTL	Functional Requirement related to Operations. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None	None Identified	N/A				1						1								1	N/C				
2.6.3.5 Machine-readable part contains same information as human-readable part	If a non-human-readable encoding is used on the paper record, it SHALL contain the entirety of the human-readable information on the record.	Inspection	VSTL	Functional Requirement related to Operations and loosely to encryption. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None	None Identified	N/A			1	1						1								1	N/C				
2.6.3.6 Format for paper record non-human-readable data	Any non-human-readable information on the paper record SHALL be presented in a non-proprietary format.	Inspection	VSTL	Functional Requirement related to Operations and loosely to encryption. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None	None Identified	N/A			1	1	1					1								1	N/C				
2.6.3.7 Linking the electronic CVR to the paper record	The paper record SHALL: a. Contain the paper record identifier; and b. Identify whether the paper record represents the ballot that was cast.	Inspection	VSTL	Functional Requirement related to Operations. No specific security control identified.	T=TEST & Demonstration	None	None	None	None	None	None	None	None Identified	N/A				1						1								1	N/C				
2.7.1.1 Network monitoring	The system server SHALL provide for system and network monitoring during the voting period.	Functional	VSTL	Functional Requirement related to Network Monitoring and Audit capability.	D=DEMONSTRATION	SI-4	Information System Monitoring Tools and Techniques	10.6.2; 10.10.1; 10.10.2; 10.10.4	11.2.5; 11.2.6	---	EBBD-1; EBVC-1; ECID-1	4.B.2.a(5)(b) ; 4.B.3.a(8)(b) ; 6.B.3.a(8)	Supplemental Guidance: The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities. Control Enhancements: (1) The organization interconnects and configures individual intrusion detection tools into a systemwide intrusion detection system using common protocols. (2) The organization employs automated tools to support near-real-time analysis of events. (3) The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination. (4) The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.	Control: The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.	1	1	1						1														IDS/IPS systems SHALL be used that actively monitors, detects, and notifies administrators of any potential malicious activity.
2.7.1.2 Tool access	The system and network monitoring functionality SHALL only be accessible to authorized personnel from restricted consoles.	Functional	VSTL	Functional and Technical security requirement related to access controls and Roles and Responsibilities.	D=DEMONSTRATION	SI-4	PS-6	Access Agreements	6.1.5; 8.1.3	6.1.5; 6.2.2	SP-4.1	PRRB-1	E2.1.44. Privileged User. An authorized user who has access to system control, monitoring, or administration functions.PRRB-1 - Security Rules of Behavior or Acceptable Use Policy A set of rules that describe the IA operations of the DoD information system and clearly delineate IA responsibilities and expected behavior of all personnel is in place. The rules include the consequences of inconsistent behavior or non-compliance. Signed acknowledgement of the rules is a condition of access.	N/A		1	1	1					1								1	N/C					
2.7.1.3 Tool privacy	System and network monitoring functionality SHALL NOT have the capability to compromise voter privacy or election integrity.	Functional	VSTL	Functional Requirement related to voter privacy and Integrity.	D=DEMONSTRATION	None	None	None	None	None	None	None		No reference documentation identified.		1	1								1							1	N/C				
4.1.1 Acceptable Programming Language Constructs	Application logic SHALL be produced in a high-level programming language that has all of the following control constructs: a. Sequence; b. Loop with exit condition (e.g., for, while, and/or do-loops); c. If/Then/Else conditional; d. Case conditional; and e. Block-structured exception handling (e.g., try/throw/catch).	Inspection	Manufacturer	Integrity: Error Handling and system logic could jeopardize confidentiality, integrity and/or availability of the voting system.	I=INSPECTION	SI-11 SI-10	Error Handling Information Accuracy, Completeness, Validity, and Authenticity	12.2.1; 12.2.2; 12.2.3; 12.2.4; 10.7.3; 12.2.1; 12.2.2	---	---	---	2.B.4.d 7.B.2.h; 2.B.4.d	ERROR HANDLING: Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries. NIST Special Publications 800-44, 800-57	N/A				1						1							1	N/C					
4.2.1 Acceptable Coding Conventions	Application logic SHALL adhere to (or be based on) a published, credible set of coding rules, conventions or standards (herein simply called "coding conventions") that enhance the workmanship, security, integrity, testability, and maintainability of applications.	Inspection	Manufacturer	Integrity: Relates to software integrity	I=INSPECTION	None	None	None	None	None	DCSQ-1 Software Quality	None	DCSQ-1 Software Quality: Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives.	N/A				1							1						1	N/C					

4.2.1.1 Published	Coding conventions SHALL be considered published if they appear in publicly available media.	Inspection	Manufacturer	Integrity: Relates to software integrity	I=INSPECTIO N	None	None	None	None	None	DCSQ-1 Software Quality	None	DCSQ-1 Software Quality: Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives.	N/A			1						1					1	N/C
4.2.1.2 Credible	Coding conventions SHALL be considered credible if at least two different organizations independently decided to adopt them and made active use of them at some time within the three years before conformity assessment was first sought.	Inspection	Manufacturer	Relates to software integrity	I=INSPECTIO N	None	None	None	None	None	DCSQ-1 Software Quality	None	DCSQ-1 Software Quality: Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives.	N/A	1	1	1						1					1	N/C
4.3.1.2 Module testability	Each module SHALL have a specific function that can be tested and verified independently from the remainder of the code.	Inspection	Manufacturer	Relates to software integrity	I=INSPECTIO N	None	None	None	None	None	None	None	None	No reference documentation identified.			1					1					1	1	N/C
4.3.1.3 Module size and identification	Modules SHALL be small and easily identifiable.	Inspection	Manufacturer	Relates to software integrity	I=INSPECTIO N	None	None	None	None	None	None	None	Nonme	N/A			1					1					1	1	N/C
4.4.1.1 Exception handling	Application logic SHALL handle exceptions using block-structured exception handling constructs.	Inspection	Manufacturer	Relates to software integrity and quality	I=INSPECTIO N	SI-11 SI-10	Error Handling Information Accuracy, Completeness, Validity, and Authenticity	12.2.1; 12.2.2; 12.2.3; 12.2.4; 10.7.3; 12.2.1; 12.2.2	---	---	---	2.B.4.d 7.B.2.h; 2.B.4.d	ERROR HANDLING: Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries. NIST Special Publications 800-44, 800-57	N/A			1	1				1				1			N/C
4.4.1.2 Legacy library units must be wrapped	If application logic makes use of any COTS or third-party logic callable units that do not throw exceptions when exceptional conditions occur, those callable units SHALL be wrapped in callable units that check for the relevant error conditions and translate them into exceptions, and the remainder of application logic SHALL use only the wrapped version.	Inspection	Manufacturer	Relates to software integrity, quality and error handling of third party software	I=INSPECTIO N	SI-7 SI-10	Software and Information Integrity	12.2.1; 12.2.2; 12.2.4	11.2.1; 11.2.4	---	ECSD-2	4.B.1.c(2); 5.B.1.a(3); 5.B.2.a(6)	SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY Control: The information system checks information for accuracy, completeness, validity, and authenticity. Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.	N/A			1	1				1				1			N/C
4.4.2 Unstructured Control Flow is Prohibited	Application logic SHALL contain no unstructured control constructs.	Inspection	Manufacturer	Relates to software integrity and quality	I=INSPECTIO N	SI-11 SI-10	Error Handling Information Accuracy, Completeness, Validity, and Authenticity	12.2.1; 12.2.2; 12.2.3; 12.2.4; 10.7.3; 12.2.1; 12.2.2	---	---	---	2.B.4.d 7.B.2.h; 2.B.4.d	ERROR HANDLING: Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries. NIST Special Publications 800-44, 800-57	N/A			1	1					1		1	1			N/C
4.4.2.1 Branching	Arbitrary branches (a.k.a. GoTos) SHALL NOT be allowed.	Inspection	Manufacturer	Relates to software integrity, quality and error handling of third party software	I=INSPECTIO N	SI-7 SI-10	Software and Information Integrity	12.2.1; 12.2.2; 12.2.4	11.2.1; 11.2.4	---	ECSD-2	4.B.1.c(2); 5.B.1.a(3); 5.B.2.a(6)	SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY Control: The information system checks information for accuracy, completeness, validity, and authenticity. Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.	N/A			1	1				1				1			N/C
4.4.2.2 Intentional exceptions	Exceptions SHALL only be used for abnormal conditions. Exceptions SHALL NOT be used to redirect the flow of control in normal ("non-exceptional") conditions.	Inspection	Manufacturer	Relates to software integrity, quality and error handling of third party software	I=INSPECTIO N	SI-7 SI-10	Software and Information Integrity	12.2.1; 12.2.2; 12.2.4	11.2.1; 11.2.4	---	ECSD-2	4.B.1.c(2); 5.B.1.a(3); 5.B.2.a(6)	SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY Control: The information system checks information for accuracy, completeness, validity, and authenticity. Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.	N/A			1	1				1				1			N/C
4.4.2.3 Unstructured exception handling	Unstructured exception handling (e.g., On Error GoTo, setjmp/longjmp) SHALL NOT be allowed.	Inspection	Manufacturer	Relates to software integrity, quality and error handling of third party software	I=INSPECTIO N	SI-7 SI-10	Software and Information Integrity	12.2.1; 12.2.2; 12.2.4	11.2.1; 11.2.4	---	ECSD-2	4.B.1.c(2); 5.B.1.a(3); 5.B.2.a(6)	SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY Control: The information system checks information for accuracy, completeness, validity, and authenticity. Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.	N/A		1	1	1				1				1			N/C
4.4.2.4 Separation of code and data	Application logic SHALL NOT compile or interpret configuration data or other input data as a programming language.	Inspection	Manufacturer	Relates to software integrity and quality	I=INSPECTIO N	SI-9	Information Input Restrictions	12.2.1; 12.2.2	---	SD-1	---	2.B.9.b(11)	SI-9 INFORMATION INPUT RESTRICTIONS Control: The organization restricts the capability to input information to the information system to authorized personnel. Supplemental Guidance: Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.	N/A			1	1					1				1		N/C
4.5.1 Header Comments	Application logic modules SHALL include header comments that provide at least the following information for each callable unit (e.g., function, method, operation, subroutine, procedure.): a. The purpose of the unit and how it works (if not obvious); b. A description of input parameters, outputs and return values, exceptions thrown, and side-effects; and c. Any protocols that must be observed (e.g., unit calling sequences).	Inspection	Manufacturer	Relates to software integrity and quality	I=INSPECTIO N	None	None	None	None	None	None	None	SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY Control: The information system checks information for accuracy, completeness, validity, and authenticity. Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.	N/A			1	1				1				1			N/C
4.6.1 Code Coherency	Application logic SHALL conform to the following sub-requirements: a. Self-modifying code SHALL NOT be allowed; b. Application logic SHALL be free of race conditions, deadlocks, livelocks, and resource starvation; c. If compiled code is used, it SHALL only be compiled using a COTS compiler; and d. If interpreted code is used, it SHALL only be run under a specific, identified version of a COTS runtime interpreter.	Inspection	Manufacturer	Relates to mobile code and best coding practices to prevent error that could impact system availability, integrity and confidentiality. This also implies that code support IA robustness requirements.	I=INSPECTIO N	SI-7	Software and Information Integrity	12.2.1; 12.2.2; 12.2.4	11.2.1; 11.2.4	---	ECSD-2	4.B.1.c(2); 5.B.1.a(3); 5.B.2.a(6)	SI-7: SOFTWARE AND INFORMATION INTEGRITY Control: The information system detects and protects against unauthorized changes to software and information. Supplemental Guidance: The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.	N/A			1	1					1			1			N/C
4.6.2 Prevent Tampering With Code	Programmed devices SHALL defend against replacement or modification of executable or interpreted code.	Inspection	Manufacturer	Relates to mobile code and best coding practices to prevent error that could impact system availability, integrity and confidentiality. This also implies that code support IA robustness requirements.	I=INSPECTIO N	SI-7	Software and Information Integrity	12.2.1; 12.2.2; 12.2.4	11.2.1; 11.2.4	---	ECSD-2	4.B.1.c(2); 5.B.1.a(3); 5.B.2.a(6)	SI-7: SOFTWARE AND INFORMATION INTEGRITY Control: The information system detects and protects against unauthorized changes to software and information. Supplemental Guidance: The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts. NIST Special Publication 800-83 provides guidance on detecting malware-based attacks through malicious code protection software.	N/A		1	1					1				1			N/C
4.6.3 Prevent Tampering With Data	The voting system SHALL prevent access to or manipulation of configuration data, vote data, or audit records.	Inspection	Manufacturer	Relates to audit capabilities and configuration management and data integrity.	I=INSPECTIO N	AU-1	Audit and Accountability Policy and Procedures	10.10; 15.1.1	17	---	ECAT-1; ECTB 1; DCAR-1	DCID: B.2.d; Manual: 2.B.4.e(5); 2.B.2.a(4)	N/A			1	1					1					1		N/C

4.7.1.1 Validity check	Programmed devices SHALL check information inputs for completeness and validity.	Inspection	Manufacturer	Relates to the accuracy of information and integrity of data.	I=INSPECTIO N	SI-10	Information Accuracy, Completeness, Validity, and Authenticity	10.7.3; 12.2.1; 12.2.2	---	---	FVAP UOCA	7.B.2.h; 2.B.4.d	N/A		1							1	1					N/C	4/2/2015		
4.7.1.2 Defend against garbage input	Programmed devices SHALL ensure that incomplete or invalid inputs do not lead to irreversible error.	Inspection	Manufacturer	Functional requirement and Error handling	I=INSPECTIO N	SI-11	Error Handling	12.2.1; 12.2.2; 12.2.3; 12.2.4	---	---	---	2.B.4.d	N/A		1	1					1		1						N/C		
4.7.2.1 Error checking	Application logic that is vulnerable to the following types of errors SHALL check for these errors at run time and respond defensively (as specified by Requirement 4.7.2.8) when they occur: Out-of-bounds accesses of arrays or strings (includes buffers used to move data); Stack overflow errors; CPU-level exceptions such as address and bus errors, dividing by zero, and the like; Variables that are not appropriately handled when out of expected boundaries; Numeric overflows; and Known programming language specific vulnerabilities.	Inspection	Manufacturer	Relates to the accuracy of information and integrity of data.	I=INSPECTIO N	SI-11	Error Handling	12.2.1; 12.2.2; 12.2.3; 12.2.4	---	---	---	2.B.4.d	N/A		1	1					1		1						N/C		
4.7.2.2 Range checking of indices	If the application logic uses arrays, vectors, character sequences, strings or any analogous data structures, and the programming language does not provide automatic run-time range checking of the indices, the indices SHALL be rangedchecked on every access.	Inspection	Manufacturer	Relates to the accuracy of information and integrity of data.	I=INSPECTIO N	SI-11	Error Handling	12.2.1; 12.2.2; 12.2.3; 12.2.4	---	---	---	2.B.4.d	N/A		1							1	1							N/C	
4.7.2.3 Stack overflows	If stack overflow does not automatically result in an exception, the application logic SHALL explicitly check for and prevent stack overflow.	Inspection	Manufacturer	Relates to the accuracy of information and integrity of data.	I=INSPECTIO N	SI-11	Error Handling	12.2.1; 12.2.2; 12.2.3; 12.2.4	---	---	---	2.B.4.d	N/A		1							1	1							N/C	
4.7.2.4 CPU traps	The application logic SHALL implement such handlers as are needed to detect and respond to CPU-level exceptions including address and bus errors and dividing by zero.	Inspection	Manufacturer	Relates to the accuracy of information and integrity of data.	I=INSPECTIO N	SI-11	Error Handling	12.2.1; 12.2.2; 12.2.3; 12.2.4	---	---	---	2.B.4.d	N/A		1	1					1		1						N/C		
4.7.2.5 Garbage input parameters	All scalar or enumerated type parameters whose valid ranges as used in a callable unit (e.g., function, method, operation, subroutine, procedure.) do not cover the entire ranges of their declared data types SHALL be range-checked on entry to the unit.	Inspection	Manufacturer	Relates to error handling and data range values.	I=INSPECTIO N	SI-10	Information Accuracy, Completeness, Validity, and Authenticity	10.7.3; 12.2.1; 12.2.2	---	---	---	7.B.2.h; 2.B.4.d	N/A		1						1		1						N/C		
4.7.2.6 Numeric overflows	If the programming language does not provide automatic run-time detection of numeric overflow, all arithmetic operations that could potentially overflow the relevant data type SHALL be checked for overflow.	Inspection	Manufacturer	Integrity: Relates to error handling and data range values.	I=INSPECTIO N	SI-10	Information Accuracy, Completeness, Validity, and Authenticity	10.7.3; 12.2.1; 12.2.2	---	---	---	7.B.2.h; 2.B.4.d	N/A		1						1		1						N/C		
4.7.2.7 Nullify freed pointers	If pointers are used, any pointer variables that remain within scope after the memory they point to is deallocated SHALL be set to null or marked as invalid (pursuant to the idiom of the programming language used) after the memory they point to is deallocated.	Inspection	Manufacturer	Integrity and Availability: Relates to software quality and best programming practices. No specific security control.	I=INSPECTIO N	None	None	None	None	None	None	None	None	None	1	1					1					1			N/C		
4.7.2.8 React to errors detected	The detection of any of the errors enumerated in Requirement 4.7.2.1 SHALL be treated as a complete failure of the callable unit in which the error was detected. An appropriate exception SHALL be thrown and control SHALL pass out of the unit forthwith.	Inspection	Manufacturer	Integrity and Availability: Relates to software quality and best programming practices. No specific security control.	I=INSPECTIO N	SI-11	Error Handling	12.2.1; 12.2.2; 12.2.3; 12.2.4	---	---	---	2.B.4.d	None	N/A		1	1				1						1			N/C	

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

4.9.2.1 Security control source code review	The test lab SHALL analyze the source code of the security controls to assess whether they function correctly and cannot be bypassed.	Inspection	VSTL	Loss of Integrity, availability and/or Confidentiality	I=INSPECTION	RA-5	Vulnerability Scanning	12.6.1	10.3.2; 14.2.1	---	ECMT-1; VIVM-1	4.B.3.a(8)(b); 4.B.3.b(6)(b); 9.B.4.e	RA-5: VULNERABILITY SCANNING Control: The organization scans for vulnerabilities in the information system (Assignment: organization-defined frequency) or when significant new vulnerabilities potentially affecting the system are identified and reported. Supplemental Guidance: Vulnerability scanning is conducted using appropriate scanning tools and techniques. The organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques. Vulnerability scans are scheduled and/or random in accordance with organizational policy and assessment of risk. The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems. Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools for applications, source code reviews, static analysis of source code). NIST Special Publication 800-42 provides guidance on network security testing. NIST Special Publication 800-40 (Version 2) provides guidance on patch and vulnerability management.	N/A	1	1	1				1	1					4/2/2015	Recommend the use of application scanning tools such as Lumension, Nessus or Fortify for source code analysis.
5.1.1.1 Definition of roles	The voting system SHALL allow the definition of personnel roles with segregated duties and responsibilities on critical processes to prevent a single person from compromising the integrity of the system.	Functional	VSTL	Relates to the separation of duties, least privilege and account management. Roles and Responsibilities are discussed in many different sections. Impacts include: Loss of Confidentiality, Availability and Integrity. This is an operating system functional requirement to meet the above.	D=DEMONSTRATION	AC-2	Account Management	6.2.2; 6.2.3; 8.3.3; 11.2.1; 11.2.2; 11.2.4; 11.7.2	6.1.8; 15.1.1; 15.1.4; 15.1.5; 15.1.8; 15.2.2; 16.1.3; 16.1.5; 16.2.12	AC-2.1; AC-2.2; AC-3.2; SP-4.1	IAAC-1	4.B.2.a(3)	ECLP-1 Least Privilege Access procedures enforce the principles of separation of duties and "least privilege." Access to privileged accounts is limited to privileged users. Use of privileged accounts is limited to privileged functions; that is, privileged users use non-privileged accounts for all non-privileged functions. This control is in addition to an appropriate security clearance and need-to-know authorization.	N/A	1	1	1				1	1					Recommend the use of application scanning tools such as Lumension, Nessus or Fortify for source code analysis.	
5.1.1.2 Access to election data	The voting system SHALL ensure that only authorized roles, groups, or individuals have access to election data.	Functional	VSTL	Relates to the separation of duties, least privilege and account management. Roles and Responsibilities are discussed in many different sections. Impacts include: Loss of Confidentiality, Availability and Integrity. This is an operating system functional requirement to meet the above.	D=DEMONSTRATION	AC-2	Account Management	6.2.2; 6.2.3; 8.3.3; 11.2.1; 11.2.2; 11.2.4; 11.7.2	6.1.8; 15.1.1; 15.1.4; 15.1.5; 15.1.8; 15.2.2; 16.1.3; 16.1.5; 16.2.12	AC-2.1; AC-2.2; AC-3.2; SP-4.1	IAAC-1	4.B.2.a(3)		N/A	1	1	1				1	1					Recommend the use of application scanning tools such as Lumension, Nessus or Fortify for source code analysis.	
5.1.1.3 Separation of duties	The voting system SHALL require at least two persons from a predefined group for validating the election configuration information, accessing the cast vote records, and starting the tabulation process.	Functional	VSTL	Integrity & Confidentiality: Procedural requirement to prevent collusion	D=DEMONSTRATION	AC-4	Information Flow Enforcement	10.6.2; 11.4.5; 11.4.6; 11.4.7	---	---	EBBD-1; EBBD-2	4.B.3.a(3); 7.B.3.g	AC-5 SEPARATION OF DUTIES Control: The information system enforces separation of duties through assigned access authorizations. Supplemental Guidance: The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.	N/A	1	1	1				1	1					N/C	
5.1.2.1 Identity verification	The voting system SHALL identify and authenticate each person to whom access is granted, and the specific functions and data to which each person holds authorized access.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	AC-7	Unsuccessful Login Attempts	11.5.1	15.1.14	AC-3.2	ECLO-1	4.B.2.a(17)(c)-(d)		N/A	1	1	1				1	1					N/C	
5.1.2.2 Access control configuration	The voting system SHALL allow the administrator group or role to configure permissions and functionality for each identity, group or role to include account and group/role creation, modification, and deletion.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	AC-5	Separation of Duties	10.1.3; 10.6.1; 10.10.1	6.1.1; 6.1.2; 6.1.3; 15.2.1; 16.1.2; 17.1.5	AC-3.2; SD-1.2	ECLP-1	2.A.1; 4.B.3.a(18)	AC-5 SEPARATION OF DUTIES Control: The information system enforces separation of duties through assigned access authorizations. Supplemental Guidance: The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.	N/A	1	1	1				1	1					N/C	
5.1.2.3 Default access control configuration	The voting system's default access control permissions SHALL implement the least privileged role or group needed.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	AC-5	Separation of Duties	10.1.3; 10.6.1; 10.10.1	6.1.1; 6.1.2; 6.1.3; 15.2.1; 16.1.2; 17.1.5	AC-3.2; SD-1.2	ECLP-1	2.A.1; 4.B.3.a(18)	AC-5 SEPARATION OF DUTIES Control: The information system enforces separation of duties through assigned access authorizations. Supplemental Guidance: The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.	N/A	1	1	1				1	1					N/C	
5.1.2.4 Escalation prevention	The voting system SHALL prevent a lower-privilege process from modifying a higher-privilege process.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	AC-5	Separation of Duties	10.1.3; 10.6.1; 10.10.1	6.1.1; 6.1.2; 6.1.3; 15.2.1; 16.1.2; 17.1.5	AC-3.2; SD-1.2	ECLP-1	2.A.1; 4.B.3.a(18)	SC-3 SECURITY FUNCTION ISOLATION Control: The information system isolates security functions from nonsecurity functions. Supplemental Guidance: The information system isolates security functions from nonsecurity functions by means of partitions, domains, etc., including control of access to and integrity of, the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (e.g., address space) for each executing process.	N/A	1	1	1				1	1					N/C	

[illegible]

5.2.1.1 Strength of authentication	Authentication mechanisms supported by the voting system SHALL support authentication strength of at least 1/1,000,000.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	IA-2	User Identification and Authentication	11.2.3; 11.4.2; 11.5.2	15.1	---	IAIA-1	4.B.2.a(7)	USER IDENTIFICATION AND AUTHENTICATION Control: The information system uniquely identifies and authenticates users (or processes acting on behalf of users). Supplemental Guidance: Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance security control AC-14. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. NIST Special Publication 800-63 provides guidance on remote electronic authentication including strength of authentication mechanisms.	N/A	1	1	1				1		1						4/2/2015 Recommendation: The use of three factor authentication method to include biometric. Cross-over error rates (CER) and Equal Error Rates should be known.
5.2.1.2 Minimum authentication methods	The voting system SHALL authenticate users per the minimum authentication methods outlined below.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	IA-2	User Identification and Authentication	11.2.3; 11.4.2; 11.5.2	15.1	---	IAIA-1	4.B.2.a(7)	IA-2 USER IDENTIFICATION AND AUTHENTICATION Control: The information system uniquely identifies and authenticates users (or processes acting on behalf of users). Supplemental Guidance: Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance security control AC-14. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof.	N/A	1	1	1				1		1						N/C
5.2.1.3 Multiple authentication mechanisms	The voting system SHALL provide multiple authentication methods to support multi-factor authentication.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	IA-2	User Identification and Authentication	11.2.3; 11.4.2; 11.5.2	15.1	---	IAIA-1	4.B.2.a(7)	IA-2 USER IDENTIFICATION AND AUTHENTICATION Control: The information system uniquely identifies and authenticates users (or processes acting on behalf of users). Supplemental Guidance: Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance security control AC-14. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof.	N/A	1	1	1				1		1						N/C
5.2.1.4 Secure storage of authentication data	When private or secret authentication data is stored by the voting system, it SHALL be protected to ensure that the confidentiality and integrity of the data are not violated.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	D=DEMONSTRATION	IA-5	Authenticator Management	11.5.2; 11.5.3	15.1.6; 15.1.7; 15.1.9; 15.1.10; 15.1.11; 15.1.12; 15.1.13; 16.1.3; 16.2.3	AC-3.2	IAKM-1; IATS-1; IAIA-2	4.B.2.a(7); 4.B.3.a(11)	IA-5 AUTHENTICATOR MANAGEMENT Control: The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically. Supplemental Guidance: Information system authenticators include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. For password-based authentication, the information system: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations.	N/A	1	1				1		1						N/C	
5.2.1.5 Password reset	The voting system SHALL provide a mechanism to reset a password if it is forgotten, in accordance with the system access/security policy.	Functional	VSTL	Passwords, tokens, or other devices are used to identify and authenticate users. Loss of Integrity, Availability and Confidentiality	D=DEMONSTRATION	IA-5	Authenticator Management	11.5.2; 11.5.3	15.1.6; 15.1.7; 15.1.9; 15.1.10; 15.1.11; 15.1.12; 15.1.13; 16.1.3; 16.2.3	AC-3.2	IAKM-1; IATS-1	4.B.2.a(7); 4.B.3.a(11)	Related security controls: AC-14, AC-17	N/A	1	1				1		1						N/C	
5.2.1.6 Password strength configuration	The voting system SHALL allow the administrator group or role to specify password strength for all accounts including minimum password length, use of capitalized letters, use of numeric characters, and use of non-alphanumeric characters per NIST 800-63 Electronic Authentication Guideline Standards.	Functional	VSTL	Medium Impact. Administrative roles and responsibilities	D=DEMONSTRATION	IA-5	Authenticator Management	11.5.2; 11.5.3	15.1.6; 15.1.7; 15.1.9; 15.1.10; 15.1.11; 15.1.12; 15.1.13; 16.1.3; 16.2.3	AC-3.2	IAKM-1; IATS-1	4.B.2.a(7); 4.B.3.a(11)	IA-5 AUTHENTICATOR MANAGEMENT Control: The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.	N/A	1	1				1		1						N/C	
5.2.1.7 Password history configuration	The voting system SHALL enforce password histories and allow the administrator to configure the history length when passwords are stored by the system. 1 NIST Special Publication 800-57	Functional	VSTL	Medium: Impacts Integrity.	D=DEMONSTRATION	IA-5	Authenticator Management	11.5.2; 11.5.3	15.1.6; 15.1.7; 15.1.9; 15.1.10; 15.1.11; 15.1.12; 15.1.13; 16.1.3; 16.2.3	AC-3.2	IAKM-1; IATS-1	4.B.2.a(7); 4.B.3.a(11)	IA-5 AUTHENTICATOR MANAGEMENT Control: The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.	N/A	1	1				1		1						N/C	
5.2.1.8 Account information password restriction	The voting system SHALL ensure that the user name is not used in the password.	Functional	VSTL	Medium: Impacts Integrity.	D=DEMONSTRATION	IA-5	Authenticator Management	11.5.2; 11.5.3	15.1.6; 15.1.7; 15.1.9; 15.1.10; 15.1.11; 15.1.12; 15.1.13; 16.1.3; 16.2.3	AC-3.2	IAKM-1; IATS-1	4.B.2.a(7); 4.B.3.a(11)	IA-5 AUTHENTICATOR MANAGEMENT Control: The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.	N/A	1	1				1		1						N/C	
5.2.1.9 Automated password expiration	The voting system SHALL provide a means to automatically expire passwords.	Functional	VSTL	Medium: Impacts Integrity.	D=DEMONSTRATION	IA-5	Authenticator Management	11.5.2; 11.5.3	15.1.6; 15.1.7; 15.1.9; 15.1.10; 15.1.11; 15.1.12; 15.1.13; 16.1.3; 16.2.3	AC-3.2	IAKM-1; IATS-1	4.B.2.a(7); 4.B.3.a(11)	IA-5 AUTHENTICATOR MANAGEMENT Control: The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.	N/A	1	1				1		1						Passwords SHALL conform to DoD DIACAP minimum standards.	
5.2.1.10 Device authentication	The voting system servers and vote capture devices SHALL identify and authenticate one another using NIST - approved cryptographic authentication methods at the 112 bits of security.	Functional	VSTL	Medium: Impacts Integrity.	D=DEMONSTRATION	CA-3	Information System Connections	10.6.2; 10.9.1; 11.4.5; 11.4.6; 11.4.7	1.1.1; 3.2.9; 4.1.8; 12.2.3	CC-2.1	DCID-1; EBCR-1; EBRU-1; EBPW-1; ECIC-1	9.B.3; 9.D.3.c	CA-3 INFORMATION SYSTEM CONNECTIONS Control: The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.	N/A	1	1				1		1						N/C	

Page 10 of 23

Version 2.1

5.3.2.4 Use NIST-approved key generation methods for communications	Cryptographic keys used to protect information in-transit over public telecommunication networks SHALL use NIST-approved key generation methods. If the approved key generation method requires input from a random number generator, then an approved (FIPS 140-2) random number generator SHALL be used.	Inspection	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST	SC-12	Cryptographic Key Establishment and Management	12.3.1; 12.3.2	16.1.7; 16.1.8	---	FVAP UOCA IAKM-1	1.G	National Institute of Standards and Technology Special Publication 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised), March 2007.SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT Control: When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures. Supplemental Guidance: NIST Special Publication 800-56 provides guidance on cryptographic key establishment. NIST Special Publication 800-57 provides guidance on cryptographic key management.	N/A	1	1	1						1	1					4/2/20 N/C	
5.3.2.5 Random number generator health tests	Random number generators used to generate cryptographic keys SHALL implement one or more health tests that provide assurance that the random number generator continues to operate as intended (e.g., the entropy source is not stuck).	Inspection	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST	None	None	None	None	None	None	None	National Institute of Standards and Technology Special Publication 800-90, The health test function determines that the DRBG mechanism continues to function correctly.	Covered in NIST Special Publication 800-90	1	1	1						1	1					N/C	
5.3.3.1 Key entry and output	Secret and private keys established using automated methods SHALL be entered into and output from a voting system in encrypted form. Secret and private keys established using manual methods may be entered into or output from a system in plaintext form.	Inspection	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST	None	None	None	None	None	None	None	National Institute of Standards and Technology Special Publication 800-90, The health test function determines that the DRBG mechanism continues to function correctly.	Covered in NIST Special Publication 800-90	1	1	1						1	1					N/C	
5.3.4.1 Key storage	Cryptographic keys stored within the voting system SHALL NOT be stored in plaintext. Keys stored outside the voting system SHALL be protected from disclosure or modification.	Inspection	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST	None	None	None	None	None	None	None	National Institute of Standards and Technology Special Publication 800-90, The health test function determines that the DRBG mechanism continues to function correctly.	N/A	1	1	1						1	1					N/C	
5.3.4.2 Key zeroization	The voting system SHALL provide methods to zeroize all plaintext secret and private cryptographic keys within the system.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST	None	None	None	None	None	None	None	National Institute of Standards and Technology Special Publication 800-90, The health test function determines that the DRBG mechanism continues to function correctly.	N/A	1	1	1						1	1					N/C	
5.3.4.3 Support for rekeying	The voting system SHALL support the capability to reset cryptographic keys to new values.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST	None	None	None	None	None	None	None	National Institute of Standards and Technology Special Publication 800-90, The health test function determines that the DRBG mechanism continues to function correctly.	N/A	1	1	1						1	1					N/C	
5.4.1.1 Cast vote integrity; transmission	The integrity and authenticity of each individual cast vote SHALL be protected from any tampering or modification during transmission.	Functional	VSTL	Loss of Integrity, confidentiality or availability of information stored, processed or transmitted.	T=TEST	SC-8	Transmission Integrity	10.6.1; 10.8.1; 10.9.1	11.2.1; 11.2.4; 11.2.9; 16.2.14	AC-3.2	ECTM-1	5.B.3.a(11)	ECTM-2 Transmission Integrity Controls Good engineering practices with regards to the integrity mechanisms of COTS, GOTS, and custom developed solutions are implemented for incoming and outgoing files, such as parity checks and cyclic redundancy checks (CRCs). Mechanisms are in place to assure the integrity of all transmitted information (including labels and security parameters) and to detect or prevent the hijacking of a communication session (e.g., encrypted or covert communication channels).	N/A	1	1	1						1	1					N/C	
5.4.1.2 Cast vote integrity; storage	The integrity and authenticity of each individual cast vote SHALL be preserved by means of a digital signature during storage.	Functional	VSTL	Functional Requirement. Loss of Integrity.	T=TEST	None	None	None	None	None	None	None	Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006.	N/A		1							1	1		1			N/C	
5.4.1.3 Cast vote storage	Cast vote data SHALL NOT be permanently stored on the vote capture device.	Functional	VSTL	Functional Requirement. Loss of Integrity.	T=TEST	None	None	None	None	None	None	None	Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006.	N/A		1							1			1	1		N/C	
5.4.1.4 Electronic ballot box integrity	The integrity and authenticity of the electronic ballot box SHALL be protected by means of a digital signature.	Functional	VSTL	Functional Requirement. Loss of Integrity and/or Confidentiality.	T=TEST	None	None	None	None	None	None	None	Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), Draft March 2006.	N/A		1							1			1	1		N/C	
5.4.1.5 Malware detection	The voting system SHALL use malware detection software to protect against known malware that targets the operating system, services, and applications.	Inspection	VSTL	Loss of Integrity, Confidentiality and/or Availability.	T=TEST	SI-3 SI-4	Malicious Code Protection Information System Monitoring Tools and Techniques	10.4.1; 10.6.2; 10.10.1; 10.10.2; 10.10.4	11.1.1; 11.1.2	---	ECVP-1; VIVM-1; EBBD-1; EBVC-1; ECID-1	5.B.1.a(4); 7.B.4.b(1)	NIST Special Publication 800-61 provides guidance on detecting attacks through various types of security technologies. NIST Special Publication 800-83 provides guidance on detecting malware-based attacks through malicious code protection software. NIST Special Publication 800-92 provides guidance on monitoring and analyzing computer security event logs. NIST Special Publication 800-94 provides guidance on intrusion detection and prevention. Related security control: AC-8. National Institute of Standards and Technology Special Publication 800-83, Guide to Malware Incident Prevention and Handling, November 2005.	N/A	1	1	1					1		1						N/C
5.4.1.6 Updating malware detection	The voting system SHALL provide a mechanism for updating malware detection signatures.	Inspection	VSTL	Loss of Integrity, Confidentiality and/or Availability.	T=TEST	SI-3	Malicious Code Protection	10.4.1	11.1.1; 11.1.2	---	ECVP-1; VIVM-1	5.B.1.a(4); 7.B.4.b(1)	NIST Special Publication 800-61 provides guidance on detecting attacks through various types of security technologies. NIST Special Publication 800-83 provides guidance on detecting malware-based attacks through malicious code protection software. NIST Special Publication 800-92 provides guidance on monitoring and analyzing computer security event logs. NIST Special Publication 800-94 provides guidance on intrusion detection and prevention. Related security control: AC-8. National Institute of Standards and Technology Special Publication 800-83, Guide to Malware Incident Prevention and Handling, November 2005.	N/A	1	1	1					1		1						N/C
5.4.1.7 Validating software on kiosk voting devices	The voting system SHALL provide the capability for kiosk workers to validate the software used on the vote capture devices as part of the daily initiation of kiosk operations.	Inspection	VSTL	Functional Requirement No direct impact on security.	T=TEST	SI-6	Security Functionality Verification	---	11.2.1; 11.2.2	SS-2.2	DCSS-1	4.B.1.c(2); 5.B.2.b(2)	SI-6 SECURITY FUNCTIONALITY VERIFICATION Control: The information system verifies the correct operation of security functions [Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every [Assignment: organization-defined time-period]] and [Selection (one or more): notifies system administrator, shuts the system down, restarts the system] when anomalies are discovered. Supplemental Guidance: The need to verify security functionality applies to all security functions. For those security functions that are not able to execute automated self-tests, the organization either implements compensating security controls or explicitly accepts the risk of not performing the verification as required.	N/A		1						1	1					N/C		
5.5.1.1 Data integrity protection	Voting systems that transmit data over communications links SHALL provide integrity protection for data in transit through the generation of integrity data (digital signatures and/or message authentication codes) for outbound traffic and verification of the integrity data for inbound traffic.	Functional	VSTL	Integrity Controls for transmission. Impacts confidentiality, Availability and Integrity.	I=INSPECTION	SC-16	Transmission of Security Parameters	7.2.2; 10.8.2; 10.9.2	16.1.6	AC-3.2	ECTM-2	4.B.1.a(3)	ECTM-2 Transmission Integrity Controls Good engineering practices with regards to the integrity mechanisms of COTS, GOTS, and custom developed solutions are implemented for incoming and outgoing files, such as parity checks and cyclic redundancy checks (CRCs). Mechanisms are in place to assure the integrity of all transmitted information (including labels and security parameters) and to detect or prevent the hijacking of a communication session (e.g., encrypted or covert communication channels).	N/A		1						1	1					N/C		
5.5.1.2 TLS/SSL	Voting systems SHALL use at a minimum TLS 1.0, SSL 3.1 or equivalent protocols, including all updates to both protocols and implementations as of the date of the submission (e.g., RFC 5746 for TLS 1.0).	Functional	VSTL	Integrity Controls for transmission. Impacts confidentiality, Availability and Integrity.	T=TEST	SC-8 SC-16	Transmission Integrity	10.6.1; 10.8.1; 10.9.1	11.2.1; 11.2.4; 11.2.9; 16.2.14	AC-3.2	ECTM-1	5.B.3.a(11)	National Institute of Standards and Technology Special Publication 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations, June 2005. IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION Control: The information system identifies and authenticates specific devices before establishing a connection. Supplemental Guidance: The information system typically uses either shared known information (e.g., Media Access Control (MAC) or Transmission Control Protocol/Internet Protocol (TCP/IP) addresses) or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the FIPS 199 security categorization of the information system with higher impact levels requiring stronger authentication. NIST Special Publication 800-77 provides guidance on protecting transmission integrity using IPsec. NIST Special Publication 800-81 provides guidance on Domain Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems.	N/A	1	1						1		1						N/C

6.1 General Requirements	At a minimum, this program SHALL: a. Include procedures for specifying, procuring, inspecting, accepting, and controlling parts and raw materials of the requisite quality; b. Require the documentation of the software development process; c. Require the documentation of the hardware specification and selection process; d. Identify and enforce all requirements for: i. In-process inspection and testing that the manufacturer deems necessary to ensure proper fabrication and assembly of hardware ii. Installation and operation of software and firmware e. Include plans and procedures for post-production environmental screening and acceptance testing; and f. Include a procedure for maintaining all data and records required to document and verify the quality inspections and tests.	Inspection	Manufacturer	Integrity Controls for transmission. Impacts confidentiality, Availability and Integrity.	I=INSPECTIO N	SA-4	Acquisitions	12.1.1	3.1.6; 3.1.7; 3.1.10; 3.1.11; 3.1.12	---	FVAP UOCA DCAS-1; DCDS-1; DCIT- 1; DCMC-1	DCID: B.2.a; C.2.a; Manual: 9.B.4	SA-4 ACQUISITIONS Control: The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.	N/A	1	1	1				1		1						4/2/20	N/C
6.2 Components from Third Parties	A manufacturer who does not manufacture all the components of its voting system, but instead procures components as standard commercial items for assembly and integration into a voting system, SHALL verify that the supplier manufacturers follow documented quality assurance procedures that are at least as stringent as those used internally by the voting system manufacturer.	Inspection	Manufacturer	loss of Integrity, availability and/or Confidentiality	I=INSPECTIO N	None	None	None	None	None	None	None	Nothing found in referenced documentation. However, this may be referenced within another publication involving acquisitions.	N/A	1	1	1				1				1					N/C
6.3 Responsibility for Tests	Manufacturer SHALL be responsible for performing all quality assurance tests, acquiring and documenting test data, and providing test reports for examination by the VSTL as part of the national certification process. These reports SHALL also be provided to the purchaser upon request.	Inspection	Manufacturer	loss of Integrity, availability and/or Confidentiality	I=INSPECTIO N	None	None	None	None	None	None	None	Nothing found in referenced documentation. However, this may be referenced within another publication involving acquisitions.	N/A		1	1				1				1					N/C
6.4 Parts and Materials, Special Tests, and Examinations	In order to ensure that voting system parts and materials function properly, manufacturers SHALL: a. Select parts and materials to be used in voting systems and components according to their suitability for the intended application. Suitability may be determined by similarity of this application to existing standard practice or by means of special tests; b. Design special tests, if needed, to evaluate the part or material under conditions accurately simulating the actual voting system operating environment; and c. Maintain the resulting test data as part of the quality assurance program documentation.	Inspection	Manufacturer	loss of Integrity, availability and/or Confidentiality	I=INSPECTIO N	None	None	None	None	None	None	None	Nothing found in referenced documentation. However, this may be referenced within another publication involving acquisitions.	N/A		1	1				1			1						N/C
6.5 Quality Conformance Inspections	The manufacturer performs conformance inspections to ensure the overall quality of the voting system and components delivered to the VSTL for national certification testing and to the jurisdiction for implementation. To meet the conformance inspection requirements the manufacturer SHALL: a. Inspect and test each voting system or component to verify that it meets all inspection and test requirements for the voting system; and b. Deliver a record of tests or a certificate of satisfactory completion with each voting system or component.	Inspection	Manufacturer	No specific requirement for vendor testing identified. Loss of Integrity, availability and/or Confidentiality	I=INSPECTIO N	None	None	None	None	None	None	None	ECMT-2 Conformance Monitoring and Testing Conformance testing that includes periodic, unannounced in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures such as the DoD IAVA or other DoD IA practices is planned, scheduled, conducted, and independently validated. Testing is intended to ensure that the system's IA capabilities continue to provide adequate assurance against constantly evolving threats and vulnerabilities.	N/A		1	1				1			1						N/C
7.1.1 Configuration Management Requirements	The configuration management documentation provided for manufacturer registration SHALL be sufficient for pilot projects.	Inspection	Test Entity: EAC	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTIO N	CM-1	Configuration Management Policy and Procedures	12.4.1; 12.5.1; 15.1.1	---	---	DCCB-1; DCPR-1; DCAR-1; E3.3.8	DCID: B.2.a Manual: 2.B.4.e(5); 5.B.2.a(5)	CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	N/A		1	1				1			1						N/C
7.1.2 Audit of Configuration Management Documentation	The manufacturer SHALL provide the following documentation to the EAC for review. This documentation will be audited during the registration review which will be conducted during the pilot testing period. The items which the EAC will audit are the following: a. Application of configuration management requirements; b. Configuration management policy; c. Configuration identification; d. Baseline, promotion, and demotion procedures; e. Configuration control procedures; f. Release process; g. Configuration audits; and h. Configuration management resources.	Inspection	Test Entity: EAC	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTIO N & T=TEST	CM-1	Configuration Management Policy and Procedures	12.4.1; 12.5.1; 15.1.1	---	---	DCCB-1; DCPR-1; DCAR-1; E3.3.8	DCID: B.2.a Manual: 2.B.4.e(5); 5.B.2.a(5)	Not vendor specific CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	N/A		1	1				1			1						
7.2.1 Classification and Naming Configuration Items	Manufacturers SHALL describe the procedures and conventions used to classify configuration items into categories and subcategories, uniquely number or otherwise identify configuration items and name configuration items.	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTIO N	CM-1	Configuration Management Policy and Procedures	12.4.1; 12.5.1; 15.1.1	---	---	DCCB-1; DCPR-1; DCAR-1; E3.3.8	DCID: B.2.a Manual: 2.B.4.e(5); 5.B.2.a(5)	Not vendor specific CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	N/A		1	1				1			1						N/C
7.2.2 Versioning Conventions	When a voting system component is part of a higher level system element such as a subsystem, the manufacturer SHALL describe the conventions used to: a. Identify the specific versions of individual configuration items and sets of items that are incorporated in higher level system elements such as subsystems; b. Uniquely number or otherwise identify versions; and c. Name versions.	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTIO N	CM-1	Configuration Management Policy and Procedures	12.4.1; 12.5.1; 15.1.1	---	---	DCCB-1; DCPR-1; DCAR-1; E3.3.8	DCID: B.2.a Manual: 2.B.4.e(5); 5.B.2.a(5)	Not vendor specific CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	N/A		1	1				1			1						N/C
7.3 Baseline and Promotion Procedures	Manufacturers SHALL establish formal procedures and conventions for establishing and providing a complete description of the procedures and related conventions used to: a. Establish a particular instance of a component as the starting baseline; b. Promote subsequent instances of a component to baseline status as development progresses through to completion of the initial completed version released to the VSTL for testing; and c. Promote subsequent instances of a component to baseline status as the component is maintained throughout its life cycle until system retirement (i.e., the system is no longer sold or maintained by the manufacturer).	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTIO N	CM-2	Baseline Configuration	7.1.1; 15.1.2	1.1.1; 3.1.9; 10.2.7; 10.2.9; 12.1.4	CC-2.3; CC-3.1; SS-1.2	DCHW-1; DCSW-1	2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6)	Not vendor specific CM-2 BASELINE CONFIGURATION Control: The organization develops, documents, and maintains a current baseline configuration of the information system.	N/A	1	1	1				1			1						
7.4 Configuration Control Procedures	Configuration control is the process of approving and implementing changes to a configuration item to prevent unauthorized additions, changes or deletions. The manufacturer SHALL establish such procedures and related conventions, providing a complete description of those procedures used to: a. Develop and maintain internally developed items; b. Acquire and maintain third-party items; c. Resolve internally identified defects for items regardless of their origin; and d. Resolve externally identified and reported defects (i.e., by customers and VSTLS).	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTIO N	CM-3	Configuration Change Control	10.1.2; 10.2.3; 12.4.1; 12.5.1; 12.5.2; 12.5.3	3.1.4; 10.2.2; 10.2.3; 10.2.8; 10.2.10; 10.2.11	SS-3.2; CC-2.2	DCPR-1	2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6); 5.B.2.a(5)	Not vendor specific CM-3 CONFIGURATION CHANGE CONTROL Control: The organization authorizes, documents, and controls changes to the information system.	N/A		1	1				1			1						N/C

7.5.1 Physical Configuration Audit (PCA)	For the PCA, a manufacturer SHALL provide: a. Identification of all items that are to be a part of the pilot release; b. Specification of compiler (or choice of compilers) to be used to generate voting system executable programs; c. Identification of all hardware that interfaces with the software; d. Configuration baseline data for all hardware that is unique to the voting system; e. Copies of all software documentation intended for distribution to users, including program listings, specifications, operations manual, voter manual, and maintenance manual; f. Identification of any changes between the physical configuration of the voting system submitted for the PCA and that submitted for the Functional Configuration Audit (FCA), with a certification that any differences do not degrade the functional characteristics; and g. Complete descriptions of its procedures and related conventions used to support this audit by i. Establishing a configuration baseline of the software and hardware to be tested; and ii. Confirming whether the voting system documentation matches the corresponding system components.	Inspection	VSTL	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTIO N	CM-2	Baseline Configuration	7.1.1; 15.1.2	1.1.1; 3.1.9; 10.2.7; 10.2.9; 12.1.4	CC-2.3; CC-3.1; SS-1.2	DCHW-1; DCSW-1	2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6)	Not vendor specific CM-2 BASELINE CONFIGURATION Control: The organization develops, documents, and maintains a current baseline configuration of the information system.	N/A		1	1				1			1						4/2/20	N/C	
7.5.2 Functional Configuration Audit (FCA)	The Functional Configuration Audit is conducted by the VSTL to verify that the voting system performs all the functions described in the system documentation. Manufacturers SHALL: a. Completely describe its procedures and related conventions used to support this audit for all voting system components; and b. Provide the following information to support this audit: c. Copies of all procedures used for module or unit testing, integration testing, and system testing; d. Copies of all test cases generated for each module and integration test, and sample ballot formats or other test cases used for system tests; and e. Records of all tests performed by the procedures listed above, including error corrections and retests.	Functional / Inspection	VSTL	Configuration/Testing	I=INSPECTIO N	None	None	None	None	None	None	None		N/A		1	1	1				1						1			N/C	
8.1.1.1.1 Identify full system configuration	Manufacturers SHALL submit to the VSTL documentation necessary for the identification of the full system configuration submitted for evaluation and for the development of an appropriate test plan by the VSTL.	Inspection	Manufacturer	Documentation	I=INSPECTIO N	CM-2	Baseline Configuration	7.1.1; 15.1.2	1.1.1; 3.1.9; 10.2.7; 10.2.9; 12.1.4	CC-2.3; CC-3.1; SS-1.2	DCHW-1; DCSW-1	2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6)	DCHW-1 HW Baseline A current and comprehensive baseline inventory of all hardware (HW) (to include manufacturer, type, model, physical location and network topology or architecture) required to support enclave operations is maintained by the Configuration Control Board (CCB) and as part of the SSAA. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original.	N/A		1	1	1				1			1				1		N/C	
8.1.1.1.2 Required content for pilot certification	Manufacturers SHALL provide a list of all documents submitted controlling the design, construction, operation, and maintenance of the voting system. At minimum, the TDP SHALL contain the following documentation: Implementation statement; Voting system user documentation (See Section 9 Voting Equipment User Documentation); System hardware specification; Application logic design and specification; System security specification; System test specification; Configuration for testing; and Training documentation.	Inspection	Manufacturer	Documentation	I=INSPECTIO N	CM-2	Baseline Configuration	7.1.1; 15.1.2	1.1.1; 3.1.9; 10.2.7; 10.2.9; 12.1.4	CC-2.3; CC-3.1; SS-1.2	DCHW-1; DCSW-1	2.B.7.c(7); 4.B.1.c(3); 4.B.2.b(6)	DCHW-1 HW Baseline A current and comprehensive baseline inventory of all hardware (HW) (to include manufacturer, type, model, physical location and network topology or architecture) required to support enclave operations is maintained by the Configuration Control Board (CCB) and as part of the SSAA. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original.	N/A			1				1				1				1		N/C	
8.1.1.2.1 Table of contents and abstracts	The TDP SHALL include a detailed table of contents for the required documents, an abstract of each document, and a listing of each of the informational sections and appendices presented.	Inspection	Manufacturer	Documentation	I=INSPECTIO N	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	Hundreds of references to design and documentation requierments	N/A			1				1				1				1		N/C	
8.1.1.2.2 Cross-index	A cross-index SHALL be provided indicating the portions of the documents that are responsive to the documentation requirements enumerated in section 8.1.1.1.2.	Inspection	Manufacturer	Documentation	I=INSPECTIO N	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	Hundreds of references to design and documentation requierments	N/A			1				1				1				1		N/C	
8.1.2.1 Identify proprietary data	Manufacturers SHALL identify all documents, or portions of documents, containing proprietary information that is not releasable to the public.	Inspection	Manufacturer	Documentation	I=INSPECTIO N	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	Hundreds of references to design and documentation requierments	N/A			1	1			1				1				1		N/C	
8.2.1 TDP Implementation Statement	The TDP SHALL include an implementation statement.	Inspection	Manufacturer	Documentation	I=INSPECTIO N	None	None	None	None	None	None	None	None	N/A				1			1						1	1			N/C	
8.3.1 System Hardware Specification Scope	Manufacturers SHALL expand on the system overview included in the user documentation by providing detailed specifications of the hardware components of the voting system, including specifications of hardware used to support the telecommunications capabilities of the voting system, if applicable.	Inspection	Manufacturer	Documentation	I=INSPECTION	MA-1	System Maintenance Policy and Procedures	10.1.1; 15.1.1	10	---	PRMP-1; DCAR-1	DCID: B.2.a Manual; 2.B.4.e(5); 6.B.2.a(5)	Hundreds of references to design and documentation requierments	N/A				1			1					1			1		N/C	
8.3.2.1 Description of hardware characteristics	Manufacturers SHALL provide a detailed discussion of the characteristics of the system, indicating how the hardware meets individual requirements defined in this document, including: a. Performance characteristics: Basic system performance attributes and operational scenarios that describe the manner in which system functions are invoked, describe environmental capabilities, describe life expectancy, and describe any other essential aspects of system performance; b. Physical characteristics: Suitability for intended use, requirements for security criteria, and vulnerability to adverse environmental factors; c. Reliability: System and component reliability stated in terms of the system's operating functions, and identification of items that require special handling or operation to sustain system reliability; and d. Environmental conditions: Ability of the system to withstand natural environments, and operational constraints in normal and test environments, including all requirements and restrictions regarding electrical service, telecommunications services, environmental protection, and any additional facilities or resources required to install and operate the system.	Inspection	Manufacturer	Documentation	I=INSPECTIO N	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	Hundreds of references to design and documentation requierments	N/A		1	1	1				1				1				1		N/C
8.3.3.1 System configuration	Manufacturers SHALL provide sufficient data, or references to data, to identify unequivocally the details of the system configuration submitted for testing.	Inspection	Manufacturer	Documentation	I=INSPECTIO N	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	Hundreds of references to design and documentation requierments	N/A				1					1			1				1		N/C

[illegible]

8.4.14.3 Mixed-language software	If an application logic module is written in a programming language other than that generally used within the system, the specification for the module SHALL indicate the programming language used and the reason for the difference.	Inspection	Manufacturer	Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTIO N	SI-2	Flaw Remediation	10.10.5; 12.4.1; 12.5.1; 12.5.2; 12.6.1	10.3.2; 11.1.1; 11.1.2; 11.2.2; 11.2.7	SS-2.2	DCSQ-1; DCCT-1; VIVM-1	5.B.2.a(5)(a)(3); 6.B.2.a(5)	DCSQ-1 Software Quality Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives.	N/A	1	1	1				1		1						4/2/20 N/C
8.4.14.4 References for foreign programming languages	If a module contains embedded border logic commands for an external library or package (e.g., menu selections in a database management system for defining forms and reports, on-line queries for database access and manipulation, input to a graphical user interface builder for automated code generation, commands to the operating system, or shell scripts), the specification for the module SHALL contain a reference to user manuals or other documents that explain them.	Inspection	Manufacturer	Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTIO N	SI-2	Flaw Remediation	10.10.5; 12.4.1; 12.5.1; 12.5.2; 12.6.1	10.3.2; 11.1.1; 11.1.2; 11.2.2; 11.2.7	SS-2.2	DCSQ-1; DCCT-1; VIVM-1	5.B.2.a(5)(a)(3); 6.B.2.a(5)	DCSQ-1 Software Quality Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives.	N/A	1	1	1				1		1						N/C
8.4.14.5 Source code	For each callable unit (e.g., function, method, operation, subroutine, procedure) in application logic, border logic, and third-party logic, manufacturers SHALL supply the source code.	Inspection	Manufacturer	Loss of Availability	I=INSPECTIO N	SA-6	Software Usage Restrictions	15.1.2	10.2.10; 10.2.13	SS-3.2; SP-2.1	DCPD-1	2.B.9.b(11)	NIST SP500-209DCID 6/3 Requirement: the original (source) code must be available at any time, the code must be controlled in a configuration management process, and the code must be marked with ownership and authorship. DCPD-1 Public Domain Software Controls Binary or machine executable public domain software products and other software products with limited or no warranty, such as those commonly known as freeware or shareware are not used in DoD information systems unless they are necessary for mission accomplishment and there are no alternative IT solutions available. Such products are assessed for information assurance impacts, and approved for use by the DAA. The assessment addresses the fact that such software products are difficult or impossible to review, repair, or extend, given that the Government does not have access to the original source code and there is no owner who could make such repairs on behalf of the Government.	N/A				1			1		1						N/C
8.4.14.6 Inductive assertions	For each callable unit (e.g., function, method, operation, subroutine, procedure) in core logic, manufacturers SHALL specify: a. Preconditions and postconditions of the callable unit, including any assumptions about capacities and limits within which the system is expected to operate; and b. A sound argument (preferably, but not necessarily, a formal proof) that the preconditions and postconditions of the callable unit accurately represent its behavior, assuming that the preconditions and postconditions of any invoked units are similarly accurate.	Inspection	Manufacturer	Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTIO N	SA-8	Security Engineering Principles	12.1	3.2.1	---	DCBP-1; DCCS-1; E3.4.4	1.H.1	NIST SP500-209SA-8 SECURITY ENGINEERING PRINCIPLES Control: The organization designs and implements the information system using security engineering principles. Supplemental Guidance: NIST Special Publication 800-27 provides guidance on engineering principles for information system security. The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the system.	N/A	1	1	1				1		1						N/C
8.4.14.7 High-level constraints	Manufacturers SHALL specify a sound argument (preferably, but not necessarily, a formal proof) that the core logic as a whole satisfies each of the constraints for all cases within the aforementioned capacities and limits, assuming that the preconditions and postconditions of callable units accurately characterize their behaviors.	Inspection	Manufacturer	Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTIO N	SA-8	Security Engineering Principles	12.1	3.2.1	---	DCBP-1; DCCS-1; E3.4.4	1.H.1	NIST SP500-209SA-8 (Not in searched Documetation) SECURITY ENGINEERING PRINCIPLES Control: The organization designs and implements the information system using security engineering principles. Supplemental Guidance: NIST Special Publication 800-27 provides guidance on engineering principles for information system security. The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the system.	N/A	1	1	1				1		1						N/C
8.4.14.8 Safety of concurrency	Manufacturers SHALL specify a sound argument (preferably, but not necessarily, a formal proof) that application logic is free of race conditions, deadlocks, livelocks, and resource starvation.	Inspection	Manufacturer	Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTIO N	SC-6	Resource Priority	---	---	---	---	6.B.3.a(11)	SC-6 RESOURCE PRIORITY Control: The information system limits the use of resources by priority. Supplemental Guidance: Priority protection helps prevent a lower-priority process from delaying or interfering with the information system servicing any higher-priority process.			1	1				1		1						
8.4.15.1 System database	Manufacturers SHALL identify and provide a diagram and narrative description of the system's databases and any external files used for data input or output.	Inspection	Manufacturer	Insufficient documentation could lead to difficulties supporting the application. Loss of Availability, and/or Integrity.	I=INSPECTIO N	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	SA-5 INFORMATION SYSTEM DOCUMENTATION Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.			1	1				1		1					N/C	
8.4.15.2 Database design levels	For each database or external file, manufacturers SHALL specify the number of levels of design and the names of those levels (e.g., conceptual, internal, logical, and physical).	Inspection	Manufacturer	Software Quality: Documentation normally contained within the System Security Plan as a functional requirement, or within the user documentation. Could impact Integrity, Availability and/or Confidentiality.	I=INSPECTIO N	SA-8	Security Engineering Principles	12.1	3.2.1	---	DCBP-1; DCCS-1; E3.4.4	1.H.1	NIST SP500-209SA-8 SECURITY ENGINEERING PRINCIPLES Control: The organization designs and implements the information system using security engineering principles. Supplemental Guidance: NIST Special Publication 800-27 provides guidance on engineering principles for information system security. The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the system.	N/A	1	1	1				1		1						N/C
8.4.15.3 Database design conventions	For each database or external file, the manufacturer SHALL specify any design conventions and standards (which may be incorporated by reference) needed to understand the design.	Inspection	Manufacturer	Insufficient documentation could lead to difficulties supporting the application. Loss of Availability, and/or Integrity.	I=INSPECTIO N	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	SA-5 INFORMATION SYSTEM DOCUMENTATION Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.	N/A		1	1				1		1					N/C	
8.4.15.4 Data models	For each database or external file, manufacturers SHALL identify and describe all logical entities and relationships and how these are implemented physically (e.g., tables, files).	Inspection	Manufacturer	Insufficient documentation could lead to difficulties supporting the application. Loss of Availability, and/or Integrity.	I=INSPECTIO N	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	SA-5 INFORMATION SYSTEM DOCUMENTATION Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.	N/A		1	1				1		1					N/C	
8.4.15.5 Schemata	Manufacturers SHALL document the details of table, record or file contents (as applicable), individual data elements and their specifications, including: a. Names/identifiers; b. Data type (e.g., alphanumeric, integer); c. Size and format (such as length and punctuation of a character string); d. Units of measurement (e.g., meters, seconds e. Range or enumeration of possible values (e.g., 0–99 f. Accuracy (how correct) and precision (number of significant digits); g. Priority, timing, frequency, volume, sequencing, and other constraints, such as whether the data element may be updated and whether business rules apply; h. Security and privacy constraints; and i. Sources (setting/sending entities) and recipients (using/receiving entities).	Inspection	Manufacturer	Insufficient documentation could lead to difficulties supporting the application. Loss of Availability, and/or Integrity.	I=INSPECTIO N	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD-1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	SA-5 INFORMATION SYSTEM DOCUMENTATION Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.	N/A		1	1				1		1					N/C	

9.2.3.1 User documentation system description	The system description SHALL include written descriptions, drawings and diagrams that present: a. A description of the functional components or subsystems, (e.g., environment, election management and control, vote recording, vote conversion, reporting, and their logical relationships); b. A description of the operational environment of the system that provides an overview of the hardware, firmware, software, and communications structure; c. A description that explains each system function and how the function is achieved in the design; d. Descriptions of the functional and physical interfaces between subsystems and components; e. Identification of all COTS products (both hardware and software) included in the system and/or used as part of the system's operation, identifying the name, manufacturer, and version used for each such component; f. Communications (network) software; g. Interfaces among internal components and interfaces with external systems. For components that interface with other components for which multiple products may be used, the manufacturers SHALL identify file specifications, data objects, or other means used for information exchange, and the public standard used for such file specifications, data objects, or other means; and h. Listings of all software and firmware and associated documentation included in the manufacturer's release in the order in which each piece of software or firmware would normally be installed upon system setup and installation.	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTIO N	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD 1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	SA-5 INFORMATION SYSTEM DOCUMENTATION Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system. Supplemental Guidance: Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. When adequate information system documentation is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed.	N/A		1	1		1			1																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																															
---	--	------------	--------------	---	------------------	------	----------------------------------	--------	--	--------	---	--	--	-----	--	---	---	--	---	--	--	---	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

9.4.1.2 Access control policy	Manufacturers SHALL provide, within the user documentation, the access control policy under which the system was designed to operate.	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTION	AC-1	Access Control Policy and Procedures	11.1.1; 11.4.1; 15.1.1	15.; 16.	---	FVAP UOCA ECAN-1; ECPA-1; PRAS-1; DCAR-1	2.B.4.e(5); 4.B.1.a(1)(b)	AC-1 ACCESS CONTROL POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls. Supplemental Guidance: The access control policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.	N/A	1	1					1	1							4/2/2015 N/C
9.4.1.3 Privileged account	Manufacturers SHALL disclose and document information on all privileged accounts included on the system.	Inspection	Manufacturer	Loss of Integrity, Availability and/or Confidentiality	I=INSPECTION	AC-2	Account Management	6.2.2; 6.2.3; 8.3.3; 11.2.1; 11.2.2; 11.2.4; 11.7.2	6.1.8; 15.1.1; 15.1.4; 15.1.5; 15.1.8; 15.2.2; 16.1.3; 16.1.5; 16.2.12	AC-2.1; AC-2.2; AC-3.2; SP-4.1	IAAC-1	4.B.2.a(3)	AC-2 ACCOUNT MANAGEMENT Control: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [Assignment: organization-defined frequency, at least annually]. Supplemental Guidance: Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization identifies authorized users of the information system and specifies access rights/privileges. The organization grants access to the information system based on: (i) a valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. The organization requires proper identification for requests to establish information system accounts and approves all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. Account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' information system usage or need-to-know/need-to-share changes.	N/A	1	1	1					1							N/C
9.4.2.1 System event logging	Manufacturers SHALL provide user documentation that describes system event logging capabilities and usage.	Inspection	Manufacturer	Loss of Integrity and/or Confidentiality	I=INSPECTION	AU-2 & AU-3	Auditable Events	10.10.1	17.1.1; 17.1.2; 17.1.4	---	ECAR-3	4.B.2.a(4)(d)	AU-2 AUDITABLE EVENTS Control: The information system generates audit records for the following events: [Assignment: organization-defined auditable events]. Supplemental Guidance: The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents. NIST Special Publication 800-92 provides guidance on computer security log management.	N/A		1	1					1	1					N/C	
9.4.2.2 Log format	Manufacturers SHALL provide fully documented log format information.	Inspection	Manufacturer	Provides forensic capability in the event of data loss. Provides troubleshooting abilities.	I=INSPECTION	AU-3	Content of Audit Records	10.10.1; 10.10.4	17.1.1	---	ECAR-1; ECAR-2; ECAR-3; ECLC-1	4.B.2.a(4)(a); 4.B.2.a(5)(a)	AU-3 CONTENT OF AUDIT RECORDS Control: The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. Supplemental Guidance: Audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) user/subject identity; and (v) the outcome (success or failure) of the event. NIST Special Publication 800-92 provides guidance on computer security log management.	N/A	1	1	1			1		1					N/C		
9.4.3.1 Ballot decryption process	Manufacturers SHALL provide documentation on the proper procedures for the authorized entity to implement ballot decryption while maintaining the security and privacy of the data.	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTION	CM-1	Configuration Management Policy and Procedures	12.4.1; 12.5.1; 15.1.1	---	---	DCCB-1; DCPR-1; DCAR-1; E3.3.8	DCID: B.2.a Manual: 2.B.4.e(5); 5.B.2.a(5)	CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls. Supplemental Guidance: The configuration management policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.	N/A	1	1					1	1					N/C		
9.4.3.2 Ballot decryption key reconstruction	Manufacturers SHALL provide documentation describing the proper procedure for the authorized entity to reconstruct the election private key to decrypt the ballots.	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTION	IA-5	Authenticator Management	11.5.2; 11.5.3	15.1.6; 15.1.7; 15.1.9; 15.1.10; 15.1.11; 15.1.12; 15.1.13; 16.1.3; 16.2.3	AC-3.2	IAKM-1; IATS-1	4.B.2.a(7); 4.B.3.a(11)	IA-5 AUTHENTICATOR MANAGEMENT Control: The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.	N/A		1						1	1				N/C		
9.4.3.3 Ballot decryption key destruction	Manufacturers SHALL document when any cryptographic keys created or used by the system may be destroyed. The documentation SHALL describe how to delete keys securely and irreversibly at the appropriate time.	Inspection	Manufacturer	Loss of Confidentiality, Integrity and/or availability.	I=INSPECTION	SC-12	Cryptographic Key Establishment and Management	12.3.1; 12.3.2	16.1.7; 16.1.8	---	IAKM-1	1.G	SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT Control: When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures. Supplemental Guidance: NIST Special Publication 800-56 provides guidance on cryptographic key establishment. NIST Special Publication 800-57 provides guidance on cryptographic key management.	N/A	1	1	1					1	1				N/C		

																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																													</
--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	----

[illegible]

9.6.1.11 Communications on/off status inspection procedure	Manufacturers SHALL provide the procedures to inspect the on/off status of the communications capabilities of the vote capture device.	Inspection	Manufacturer	Medium: Loss of Integrity and/or Availability	I=INSPECTIO N	PE-4	Access Control for Transmission Medium	9.2.3	7.2.2; 16.2.9	---	---	8.D.2; 4.B.1.a(8)	PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM Control: The organization controls physical access to information system distribution and transmission lines within organizational facilities. Supplemental Guidance: Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.	N/A		1	1					1	1					4/2/2015	N/C	
9.6.1.12 Consumables quantity of vote capture device	Manufacturers SHALL provide a list of consumables associated with the vote capture device, including estimated number of usages per quantity of consumable.	Inspection	Manufacturer	No known security risk.	I=INSPECTIO N	None	None	None	None	None	None	None	No specific IA Control referenced.	None			1		1						1				N/C	
9.6.1.13 Consumable inspection procedure	Manufacturers SHALL provide the procedures to inspect the remaining amount of each consumable of the vote capture device.	Inspection	Manufacturer	No known security risk.	I=INSPECTIO N	None	None	None	None	None	None	None	No specific IA Control referenced.	None			1		1						1				N/C	
9.6.1.14 Calibration of vote capture device components nominal range	Manufacturers SHALL provide a list of components associated with the vote capture devices that require calibration and the nominal operating ranges for each component.	Inspection	Manufacturer	No known security risk.	I=INSPECTIO N	None	None	None	None	None	None	None	No specific IA Control referenced.	None		1				1					1				N/C	
9.6.1.15 Calibration of vote capture device components inspection procedure	Manufacturers SHALL provide the procedures to inspect the calibration of each component.	Inspection	Manufacturer	No known security risk.	I=INSPECTIO N	None	None	None	None	None	None	None	No specific IA Control referenced.	None		1				1					1				N/C	
9.6.1.16 Calibration of vote capture device components adjustment procedure	Manufacturers SHALL provide the procedures to adjust the calibration of each component.	Inspection	Manufacturer	Calibration could impact system Integrity	I=INSPECTIO N	CM-1	Configuration Management Policy and Procedures	12.4.1; 12.5.1; 15.1.1	---	---	DCCB-1; DCPR-1; DCAR-1; E3.3.8	DCID: B.2.a Manual: 2.B.4.e(5); 5.B.2.a(5)	CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	N/A		1	1					1							N/C	
9.6.1.17 Checklist of properties to be inspected	Manufacturers SHALL provide a checklist of other properties of the system to be inspected.	Inspection	Manufacturer	Checklists are important, but may not have direct impact on security.	I=INSPECTIO N	CM-1	Configuration Management Policy and Procedures	12.4.1; 12.5.1; 15.1.1	---	---	DCCB-1; DCPR-1; DCAR-1; E3.3.8	DCID: B.2.a Manual: 2.B.4.e(5); 5.B.2.a(5)	CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	N/A		1	1					1							N/C	
9.7.1.1 System operations manual	The system operations manual SHALL provide all information necessary for system set up and use by all personnel who administer and operate the system at the state and/or local election offices and at the kiosk locations, with regard to all system functions and operations identified in Section 9.3 System Functionality Description.	Inspection	Manufacturer	High: Loss of Integrity, Availability, and/or Confidentiality	I=INSPECTIO N	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD 1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	SA-5 INFORMATION SYSTEM DOCUMENTATION Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system. Supplemental Guidance: Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. When adequate information system documentation is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed.	N/A	1	1	1				1			1						N/C
9.7.1.2 Support training	The system operations manual SHALL contain all information that is required for the preparation of detailed system operating procedures and for the training of administrators, state and/or local election officials, election judges, and kiosk workers.	Inspection	Manufacturer	High: Loss of Integrity, Availability, and/or Confidentiality	I=INSPECTIO N	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD 1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	Nothing found about training the operators!		1	1	1					1			1				N/C	
9.7.2.1 Functions	Manufacturers SHALL provide a summary of system operating functions to permit understanding of the system's capabilities and constraints.	Inspection	Manufacturer	High: Loss of Integrity, Availability, and/or Confidentiality	I=INSPECTIO N	SA-5	Information System Documentation	10.7.4	3.2.3; 3.2.4; 3.2.8; 12.1.1; 12.1.2; 12.1.3; 12.1.6; 12.1.7	CC-2.1	DCCS-1; DCHW-1; DCID-1; DCSD 1; DCSW-1; ECND-1; DCFA-1	4.B.2.b(2); 4.B.2.b(3); 4.B.4.b(4); 9.C.3	DCSQ-1 Software Quality Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives.	N/A	1	1	1				1			1					N/C	
9.7.2.2 Roles	The roles of operating personnel SHALL be identified and related to the functions of the system.	Inspection	Manufacturer	High: Loss of Integrity, Availability, and/or Confidentiality	I=INSPECTIO N	AC-2	Account Management	6.2.2; 6.2.3; 8.3.3; 11.2.1; 11.2.2; 11.2.4; 11.7.2	6.1.8; 15.1.1; 15.1.4; 15.1.5; 15.1.8; 15.2.2; 16.1.3; 16.1.5; 16.2.12	AC-2.1; AC-2.2; AC-3.2; SP-4.1	IAAC-1	4.B.2.a(3)	DCPR-1 CM Process A configuration management (CM) process is implemented that includes requirements for: (1) Formally documented CM roles, responsibilities, and procedures to include the management of IA information and documentation; (2) A configuration control board that implements procedures to ensure a security review and approval of all proposed DoD information system changes, to include inter-connections to other DoD information systems; (3) A testing process to verify proposed configuration changes prior to implementation in the operational environment; and (4) A verification process to provide additional assurance that the CM process is working effective	N/A			1			1			1					N/C		
Totals															150	246	191	0	41	130	88	186	0	28	58	15				

NIST Security Objective	Potential Impact		
	Low	Medium	High
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. Basic Testing A test methodology that assumes no knowledge of the internal structure and implementation detail of the assessment object. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.