The U.S. Election Assistance Commission

Report to Congress on EAC's Efforts to Establish Guidelines for Remote Electronic Absentee Voting Systems

April 26, 2010

Table of Contents

1. Introduction 1

2. Overview of Activities to Establish Guidelines 5

3. Policymaking Framework 5

4. Support Electronic Blank Ballot Delivery Projects 7

5. Conduct Kiosk-Based Remote Voting Pilot Project 8

6. A Phased Approach for Additional Pilot Projects 9

7. Development of Final Guidelines 10

8. Conclusion 11

Attachment A – Relevant Sections of the Military and Overseas Voter Empowerment Act

Attachment B – Relevant Sections of the 2002 National Defense Authorization Act

Attachment C – Relevant Sections of the 2005 National Defense Authorization Act

Attachment D – EAC's Draft Voting System Pilot Program Testing and Certification Program Manual

Attachment E – EAC's Draft UOCAVA Pilot Program Testing Requirements

Attachment F – 04.23.2010 EAC Request Letter to Federal Voting Assistance Program

Attachment G – Draft NISTIR 7682, Information System Security Best Practices for UOCAVA – Supporting Systems

Roadmap for the Development of Remote Electronic Absentee Voting Guidelines

1. Introduction

This document describes the Election Assistance Commission's (EAC) activities to develop guidelines for remote electronic absentee (i.e., Internet-based) voting systems to support the voting needs of military and overseas citizens. It also contains EAC's "roadmap" for the creation of guidelines for electronic absentee voting systems. EAC created this roadmap in collaboration with the National Institute of Standards and Technology (NIST), and the Federal Voting Assistance Program (FVAP).

This report is being submitted in order to meet the requirements of Section 589(e)(2) of the National Defense Authorization Act of 2009 which requires the EAC to submit a report to Congress within one hundred eighty days of enactment of the act if "…EAC has not established electronic absentee voting guidelines" within that timeframe. To date the EAC has not established those guidelines and is therefore submitting this report in accordance with the Act.

In 2002, Congress directed the Department of Defense to carry out a demonstration project under which absent uniformed services voters would be permitted to cast ballots for the November 2004 general election through an electronic voting system.

In October of 2004, Congress allowed the Department of Defense to delay the implementation of a demonstration project "…until the first regularly scheduled general election for Federal office which occurs after the Election Assistance Commission notifies the Secretary that the Commission has established electronic absentee voting guidelines…"

In 2009, Congress passed the Military and Overseas Voters Empowerment Act (MOVE) instructing FVAP that they may run pilot programs to test the ability of new or emerging technology to better serve UOCAVA voters. MOVE goes on to mandate that should FVAP choose to run a pilot program EAC and NIST are to help support FVAP by providing best practices or standards to support the projects. In addition, MOVE reiterated the 2004 mandate from Congress requiring EAC to create guidelines to be used by FVAP for the development of a remote electronic voting system.

Since Congress first directed the EAC to work on remote electronic absentee voting standards, the agency has taken several significant steps toward that end. In FY 2008 EAC issued a report entitled *UOCAVA Voters and the Electronic Transmission of Voting Materials in Four States* and three case studies describing the experiences of states transmitting ballots electronically and using Internet voting. EAC's web site includes a section dedicated to military and overseas voters featuring links to the voting sites of every branch of the military and other useful resources. These reports, studies and resources are available at www.eac.gov.

EAC is working with NIST to provide best practices to states on the transmittal and receipt of UOCAVA voting materials, including registration information and ballots. NIST completed

the first step of the process with the issuance of the December 2008 EAC-funded report: *A Threat Analysis on UOCAVA Voting Systems.*

The NIST report provided the first extensive look at the security threats associated with current and potential electronic technologies for overseas voting and identified possible ways of mitigating these risks.

In addition, the EAC has undertaken a number of initiatives related to improving the election process for UOCAVA voters. These efforts include:

- September 21, 2004 – EAC issues Best Practices for Facilitating Voting by U.S. Citizens Covered by the Uniformed and Overseas Citizens Absentee Voting Act
- September 14, 2006 – EAC holds a public meeting in St. Louis on UOCAVA voting
- September 12, 2007 – EAC and NIST sign an Interagency Agreement under which the EAC provides NIST with an additional $500,000 for the development of draft guidelines for the use of electronic technology in military and overseas citizen absentee voting.
- September 24, 2007 – EAC hosts conference in DC on UOCAVA voting
- April 2, 2008 - EAC releases an Election Management Guidelines Quick Start Guide on UOCAVA voters
- July 2010 - *Wounded Military Personnel Civic Research Initiative*. For this initiative, the EAC is collaborating with the U.S Department of Defense Federal Voting Assistance Program to better understand the voting needs of wounded military personnel and enhance the military's election processes for supporting this important constituency. The research will result in a better understanding of how to enhance, augment, and develop voting equipment and improve election processes and voting technology needed for wounded military personnel.

Notwithstanding EAC and many other groups' efforts, UOCAVA voters still do not participate in elections at the same rate as the general population. For example, EAC's 2008 Election Day survey shows that in the 2008 General Election, approximately 1 million UOCAVA ballots were transmitted by States to overseas voters. While some 680,000 of these ballots were returned and submitted for counting by voters, over 300,000 remained unreturned, returned as undeliverable or spoiled, or were otherwise unaccounted for.

Military and overseas voters face significant challenges in receiving and returning absentee ballots in time to be counted. These challenges are the result of several factors unique to members of the military and citizens living overseas. Primarily among them are 1) delays in mailing absentee ballots to voters, 2) inherently slow postal mail delivery times, and 3) the difficulty of maintaining current addresses for voters who live other than in their voting districts and move frequently.

One solution states have explored to assist this population is to distribute election materials through alternative methods, which are intended to decrease time and make the process of obtaining and returning ballots more efficient and expedient. Many states currently transmit unmarked ballots electronically, which will become a federal legislative requirement under UOCAVA for all federal elections starting with the November 2010 general election. Some

states have also implemented targeted pilot programs to facilitate the return of marked, or voted ballots. EAC's remote electronic absentee voting guidelines will be an important tool to assist states with these efforts.

To help improve UOCAVA voter participation rates, EAC's remote electronic absentee voting guidelines will include innovative approaches tailored to this unique population, including the use of non-specific mobile computing devices[1], such as personal computers. These technologies should enable UOCAVA voters to more easily vote and return their electronic ballots. To date, security concerns have delayed the implementation of general purpose personal computers for casting electronic ballots via the Internet; however, remote electronic absentee voting systems can integrate specific security protocols intended to address these concerns. For example, DoD's Common Access Card (CAC) would provide a high level of authentication for voters. This card issued to members of the military and contains secure identification information that could be used to authenticate a voter electronically prior to voting.

The goal of this project is to develop EAC certified guidelines to aide FVAP's development of an absentee voting system to serve uniformed service voters in a demonstration project administered by the Department of Defense. In addition, the EAC hopes to provide election officials with a resource to improve services for UOCAVA voters, with the ultimate goal of improving voter participation rates in this population. This roadmap moves us closer to that goal by providing for (a) nearer-term guidance for electronic distribution of UOCAVA voting materials (b) guidelines for a manned-kiosk demonstration project which will serve as an initial step towards the development of the final guidelines and (c) guidelines for remote UOCAVA voting systems that would include the capability for electronic return of marked ballots.

EAC and its partners, FVAP and NIST, have made significant progress toward assisting election officials with providing services to UOCAVA voters. However, solutions to the challenges that face UOCAVA voters will also require a broad community effort with participation from state and local election officials, computer science researchers, experts in fields such as usability and accessibility, industry representatives, and other federal agencies charged with improving the remote UOCAVA voting process. To that end, EAC will continue to solicit input from its statutory boards and the public; and work with NIST and FVAP to ensure that the remote electronic absentee voting guidelines are considered and robust.

[1] A non-specific mobile computing device is a general-purpose machine that is designed to carry out a variety of functions one of which could be running a voting platform. An example of such a device could be a laptop computer that can be carried on troop deployments.

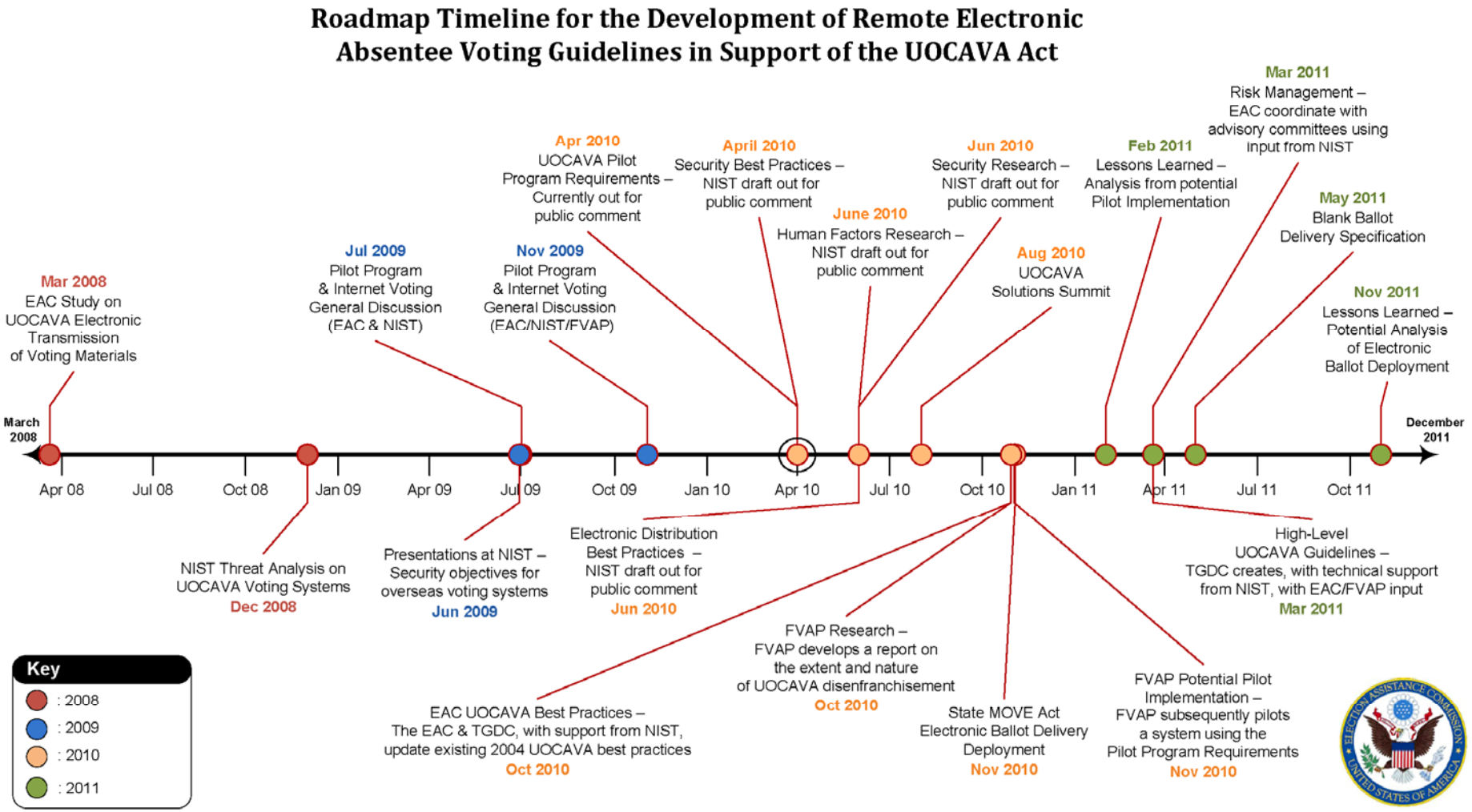


Figure 1 – Roadmap Timeline

2. Overview of Activities to Establish Guidelines

The development of remote electronic absentee voting guidelines must take into account a number of factors that are unique to this method of voting. As such, EAC intends to use a deliberative and iterative approach in the guidelines' creation and implementation which includes working closely with NIST and FVAP on the recommended steps outlined in this document. EAC has identified four major milestones in the roadmap to developing guidelines for remote electronic absentee voting. They are:

1. Perform initial research and create initial guidance including establishment of a baseline level of security assurance necessary;
2. Create a current specification for a kiosk pilot remote electronic absentee voting system to analyze the scalability and challenges posed by a multi-jurisdictional kiosk system, and to collect data on the impact of more widespread use of such a system compared to the previously modest pilot programs done in this area;
3. Identify and specify aspects of remote electronic absentee voting that election officials can implement now (e.g., blank ballot distribution); and
4. Implement a phased, iterative approach for remote electronic absentee voting pilots to determine approaches that best meet the needs of UOCAVA voters and provide adequate security precautions.

Because significant challenges to remote electronic absentee voting exist, there are also a number of interim actions outlined in this roadmap, including:

1. Facilitate sending blank ballots electronically to improve UOCAVA voter participation rates; and
2. Investigate secure platforms for transmitting electronically marked ballots for testing and pilot projects.

3. Policymaking Framework

Federal, state and local officials share responsibility for making policy decisions concerning improving UOCAVA voter participation rates through remote electronic absentee voting. Technical stakeholders -- including NIST, researchers and industry representatives -- also play an important role by providing policymakers with accurate information about challenges and possible solutions to remote electronic absentee voting. EAC will collaborate with these groups to ensure that the guidelines adequately address the factors that may impact remote electronic absentee voting, such as varying state laws, voter interests, and technological capabilities. EAC and its partners are making progress toward completing initial research and guidance; and finalizing documents that take these factors into account. EAC and its partners intend to provide ample opportunity for interested parties to participate in the development of the guidelines.

Activities:

- **April 2010** - ***Security Best Practices***: NIST will release a draft of *Information System Security Best Practices to Support UOCAVA Voting* for public comment. This document will outline some general IT best practices for securing systems that utilize the internet. These are not the same as actual electronic absentee voting guidelines, and should not be viewed as such, but may help stakeholders and the three agencies involved in this roadmap identify key requirements for the final certified guidelines.
- **May 2010** - ***FVAP Research*:** Included in its 2008 Post-Election Survey Report, FVAP will detail the extent and nature of UOCAVA voter success, the applicability of historical programs to addressing the causes of the lower success rates.
- **June 2010** - ***Electronic Distribution Best Practices*:** NIST will release a draft of *Security Best Practices for the Electronic Distribution of UOCAVA Election Materials* for public comment. This document will highlight specific steps jurisdictions can take to better secure the distribution of blank ballots or other election materials.
- **June 2010** - ***Security Research on Remote Voting***: NIST will release a draft of *Security Considerations for Remote Electronic UOCAVA Voting* for public comment. This document will focus on the security risks associated with remote electronic voting systems, including national level threats, and discuss possible mitigation of those risks.
- **June 2010** - ***Human Factors Research on Remote Voting***: NIST will release a draft of *Accessibility and Usability Considerations for Remote Electronic UOCAVA Voting* for public comment. This document will highlight steps that can be taken to make a UOCAVA remote electronic voting platform more useable and accessible for voters.
- **August 2010** - ***Research on Previous International Internet Voting Efforts:*** Australia, Estonia, the UK, and a number of other nations have already conducted numerous elections using Internet-based voting systems. These experiences can provide useful information and best practices concerning Internet-based systems in real-world elections. EAC will institute a research effort to collect and compile information from these countries to better educate stakeholders.
- **August 2010 - *UOCAVA Solutions Summit*:** NIST, EAC and FVAP will host an academic and scientific summit on the benefits and challenges of remote electronic absentee voting. Election officials, experts in computer security, and vendors of remote electronic absentee voting systems will discuss how technology can facilitate UOCAVA voters' participation. Participants will discuss desirable characteristics for remote electronic absentee voting systems by focusing on possible threats faced by remote electronic voting, approaches that can be implemented now, and technology solutions that aren't ready today but could have an impact in the future. This discussion will inform the TGDC's work on the high-level guidelines and inform the creation of a document detailing desired properties for an electronic absentee voting system which will inform the development of the final guidelines.

- **December 2010 - *EAC UOCAVA Best Practices*:** EAC and the TGDC, with technical support from NIST, will update their existing document on UOCAVA best practices for election jurisdictions to use in their efforts to better serve UOCAVA voters.
- **December 2010 - *FVAP Metrics***: Based upon FVAP's 2008 and 2009 annual reports, the NIST and EAC Best Practice documents, and the outcomes of the August 2010 Summit, FVAP will update its recommended metrics for UOCAVA voter success.
- **Spring 2011 - *High-Level Guidelines*:** EAC and the TGDC, with technical support from NIST, and input from FVAP, will identify high-level, non-testable guidelines for remote electronic absentee voting systems. This effort will focus on the desirable characteristics of such systems and serve as a needs analysis for future pilots and research; and for the purposes of driving industry to implement solutions.
- **Spring 2011 - *Risk Management*:** EAC will coordinate with its advisory boards (Board of Advisors, Standards Board, and Technical Guidelines Development Committee), and get technical input from NIST (coordinating with the Department of Defense and the National Intelligence Community, where possible), to apply the NIST Risk Management Framework and other methods in identifying security controls and technologies to mitigate security concerns. EAC will use this information to compare the current process UOCAVA voters use to vote with potential remote electronic absentee voting processes and assess the desired security protocols for both. This analysis will be used to guide future pilots and guidelines development.

4. Support Electronic Blank Ballot Delivery Projects

Some remote electronic absentee voting technologies can be implemented immediately and will likely improve UOCAVA voter participation rates. Most prominently among them is the electronic transmission of blank ballots, which allows UOCAVA voters to receive their ballots more quickly than through traditional delivery methods. Additionally, electronic registration would permit non-registered UOCAVA voters to register remotely and ultimately receive a ballot without the delays that can occur within the current framework. EAC and its partners' activities to support the wider adoption of electronic blank ballot delivery include:

Activities:

- **April 2010 - *Federal Postcard Application Wizard***: Developed by FVAP and to be available at FVAP.gov, this tool is designed to assist UOCAVA voters with filling out and submitting the Federal Post Card Application.
- **June 2010 - *Online Federal Write-in Absentee Ballot Wizard***: Developed by FVAP and to be available at FVAP.gov, this wizard is designed to assist UOCAVA voters filling out and submitting the Federal Write-in Absentee Ballot.

- **Fall 2010 - *Online Ballot Delivery and Marking Wizard***: Developed by FVAP and to be available at FVAP.gov, this wizard will provide a State-specific online ballot delivery and online marking capability for UOCAVA voters from participating states. It will still require the voter to print the ballot, hand sign and return the ballot to the appropriate jurisdiction by postal mail unless an alternative delivery technique is specifically authorized by the participating State.
- **Fall 2011 - *Common Data Format Development*:** For electronic transmission of blank ballots to be successful, they should be implemented in a manner that allows multiple states to participate. To assist in this the TGDC, with technical support from NIST, will develop common data format specifications for ballots and ballot definition that can be used by FVAP and the states. FVAP is also planning on assisting States in 2010 with data conversion services and tools to Common Data Formats.
- **Spring, 2011 - *Lessons Learned Analysis*:** After the 2010 General Election, FVAP has agreed to provide information to EAC and its advisory committees on the results of the electronic ballot delivery projects, including the success and shortcomings of their projects and lessons learned.
- **April 2011 - *Review of 2010 state activities for UOCAVA Voters:*** FVAP and EAC will review and evaluate the effectiveness of state initiatives undertaken for the 2010 Federal election related to blank ballot distribution and delivery.

5. Conduct Kiosk-Based Remote Voting Pilot Project

EAC is currently developing intermediate testable guidelines that leverage the successes achieved to date by jurisdictions with electronic absentee voting systems. These guidelines will be used to pilot remote electronic absentee voting systems implemented as a manned kiosk with printable paper ballots for audit capability. Election jurisdictions and FVAP will be able to use these guidelines to run pilot programs for UOCAVA voters should they choose to do so. The information gained from the pilot projects will be used to help inform the final guidelines development process by providing valuable information regarding the security and logistical challenges of a remote electronic voting system.

Activities:

- **April 2010 - *Testable Guidelines*:** The intermediate testable guidelines will be available for public review and subsequent update.
- **November 2010 - *Pilot Implementation*:** As indicated in the MOVE Act, FVAP or jurisdictions may choose to lead a voluntary pilot project for election jurisdictions that wish to use equipment that meets the interim testable guidelines in the General Election. The initial target for the pilot may be the 2010 general election.
- **Spring 2011 - *Lessons Learned Analysis*:** FVAP and participating election jurisdictions will provide information to EAC and its advisory committees on the results of the pilot project, including the success and shortcoming of the pilot as well as lessons learned.

6. A Phased Approach for Additional Pilot Projects

EAC, NIST and FVAP will employ a phased, iterative approach to develop guidelines tailored to the specific needs of UOCAVA voters, especially members of the military as the voter population legislatively mandated to be provided this electronic absentee voting demonstration project. The phased approach, utilizing pilot projects, allows policymakers to look at relevant technical information and implement improvements that can be deployed incrementally with existing technology. The results of the pilot projects will supply important information on what barriers have been addressed and what problems require additional research or guidelines development. Pilot projects can be conducted with existing technology that has the potential to make substantial improvements to the remote electronic absentee voting process, as well as provide important information to stakeholders working towards solutions for remote electronic absentee voting.

Activities:

- **March 2011 - *Framing the Issues*:** EAC, NIST and FVAP will provide EAC's advisory boards with background information about the legal, technical, and policy issues associated with implementing remote electronic voting systems. This includes information on security related to remote electronic absentee voting systems, potential mitigating technologies, and challenges faced by UOCAVA voters and election jurisdictions that wish to deploy new technologies.
- **Spring 2011 - *Implementation of Pilot Project:*** EAC, in consultation with its advisory boards, will consider the information described above, and structure an interim pilot project that takes existing technology--including limitations--into account. The pilot will have a specific set of stated goals that advance the guidelines and existing technology toward the goals and objectives stated in the previous section of this roadmap. Possible interim pilot projects could include:
    - Unmanned kiosk remote voting systems;
    - Remote electronic voting systems with specialized hardware, such as the Common Access Card and smartcard readers; and
    - Remote electronic voting systems without specialized hardware or software.
- **Spring 2012 - *Develop Supporting Materials*:** The TGDC, with technical support from NIST, will develop supporting materials for the pilot project. Depending on the interim pilot project, this could involve developing testable requirements, guidelines, or best practices.
- **November 2012 - *Conduct Pilot Project*:** FVAP may coordinate with state and local election jurisdictions to deploy and use a pilot system in the General Election. EAC will assist with pilot projects by utilizing its pilot certification process including the possible development of specific requirements for these pilot systems.
- **Spring, 2013 - *Lessons Learned Analysis:*** After the 2012 election, FVAP and participating jurisdictions will provide information to EAC and its advisory boards on the results of the pilot, including the success and shortcomings of the pilot and

lessons learned. The EAC through the TGDC will provide technical support to FVAP as it works to conduct these evaluations.

Additional Phases:

FVAP will compile the results of the pilot projects in the participating jurisdictions. Thereafter, EAC and its advisory boards will analyze the information to determine if the results of the pilot projects indicate that the guidelines sufficiently take into account practical considerations or another set of pilot projects is necessary. If additional phases of interim pilot projects are required, EAC, NIST and FVAP will again identify the items policymakers will need to address before additional pilots, then work to implement them.

7. Development of Final Guidelines

After collecting and synthesizing all of the information from pilot projects and conducting the necessary associated research, EAC will finalize its remote electronic absentee voting system guidelines.

Activities:

- ***Development of Guidelines***: The TGDC, with technical support from NIST, will develop draft guidelines for remote electronic absentee voting systems and submit them to EAC for consideration.
- ***Issuance of TGDC Draft Guidelines for Public Comment***: EAC will release the draft guidelines for public comment. EAC will update the public on its progress throughout the comment period at public meetings and through its newsletter.
- ***Issuance of EAC Draft Guidelines for Public Comment*:** After the completion of the public comment period for the TGDC draft version of the guidelines EAC will resolve all public comments and make appropriate policy decisions. EAC will then update the guidelines to reflect these decisions and publish the EAC draft version of the guidelines for public comment.
- ***Finalization of Guidelines:*** After the completion of the comment period on EAC's draft version of the guidelines EAC will resolve all remaining public comments and make policy decisions. EAC will then update the document to reflect those decisions and publish the final version of the guidelines.
- ***Establishment of Guidelines and Certification to Department of Defense:*** After the final publication of the guidelines, and in accordance with the 2005 National Defense Authorization Act, the EAC will notify the Secretary of Defense that the Commission has established electronic absentee voting guidelines and certify that it will assist the Secretary in carrying out the demonstration project.
- ***Deployment and Use:*** FVAP will coordinate with state and local election officials to deploy systems certified with the remote electronic absentee voting system guidelines. The process to design, develop and deploy systems to the guidelines will take 24-60 months from the availability of the certified guidelines from EAC.

8. Conclusion

EAC appreciates the opportunity to update Congress on its continuing work to improve the services for UOCAVA voters. The research, technical resources, and draft requirements EAC has produced provide the foundation for the final development of FVAP's remote electronic voting system that will improve success for UOCAVA voters.

EAC has created an iterative approach, striking a balance between protecting the privacy of the ballot, ensuring the security of the system, and instilling transparency throughout the development process. EAC looks forward to continuing to work with its partners, FVAP and NIST, as well as the public to deliver work products that produce tangible results for UOCAVA voters.

Attachment A – Relevant Sections of the Military and Overseas Voter Empowerment Act

(8) Such other recommendations for legislative or administrative action as the Secretary considers appropriate.

SEC. 573. COMPTROLLER GENERAL REPORT ON CHILD CARE ASSISTANCE FOR MEMBERS OF THE ARMED FORCES.

(a) IN GENERAL.—Not later than 18 months after the date of the enactment of this Act, the Comptroller General of the United States shall submit to the Committees on Armed Services of the Senate and the House of Representatives a report on financial assistance for child care provided by the Department of Defense to members of the Armed Forces (including members of the reserve components of the Armed Forces who are deployed in connection with a contingency operation).

(b) ELEMENTS.—The report required by subsection (a) shall include an assessment of the following:

(1) The types of financial assistance for child care made available by the Department of Defense to members of the Armed Forces (including members of the reserve components of the Armed Forces who are deployed in connection with a contingency operation).

(2) The extent to which such members have taken advantage of such assistance since such assistance was first made available.

(3) The formulas used for calculating the amount of such assistance provided to such members.

(4) The funding allocated to such assistance.

(5) The remaining costs of child care to families of such members that are not covered by the Department of Defense.

(6) Any barriers to access to such assistance faced by such members and the families of such members.

(7) The different criteria used by different States with respect to the regulation of child care services and the potential impact differences in such criteria may have on the access of such members to such assistance.

(8) The different standards and criteria used by different programs of the Department of Defense for providing such assistance with respect to child care providers and the potential impact differences in such standards and criteria may have on the access of such members to such assistance.

(9) The number of qualified families that do not receive any financial assistance for child care made available by the Department of Defense.

(10) Any other matters the Comptroller General determines relevant to the improvement of financial assistance to expand access for child care made available by the Department of Defense to members of the Armed Forces (including members of the reserve components of the Armed Forces who are deployed in connection with a contingency operation).

Subtitle H—Military Voting

SEC. 575. SHORT TITLE.

This subtitle may be cited as the "Military and Overseas Voter Empowerment Act".

SEC. 576. CLARIFICATION REGARDING DELEGATION OF STATE RESPONSIBILITIES TO LOCAL JURISDICTIONS.

Nothing in the Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973ff et seq.) may be construed to prohibit a State from delegating its responsibilities in carrying out the requirements of such Act, including any requirements imposed as a result of the provisions of and amendments made by this Act, to jurisdictions in the State.

SEC. 577. ESTABLISHMENT OF PROCEDURES FOR ABSENT UNIFORMED SERVICES VOTERS AND OVERSEAS VOTERS TO REQUEST AND FOR STATES TO SEND VOTER REGISTRATION APPLICATIONS AND ABSENTEE BALLOT APPLICATIONS BY MAIL AND ELECTRONICALLY.

(a) IN GENERAL.—Section 102 of the Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973ff–1) is amended—

(1) in subsection (a)—

(A) in paragraph (4), by striking "and" at the end;

(B) in paragraph (5), by striking the period at the end and inserting "; and"; and

(C) by adding at the end the following new paragraph:

"(6) in addition to any other method of registering to vote or applying for an absentee ballot in the State, establish procedures—

"(A) for absent uniformed services voters and overseas voters to request by mail and electronically voter registration applications and absentee ballot applications with respect to general, special, primary, and runoff elections for Federal office in accordance with subsection (e);

"(B) for States to send by mail and electronically (in accordance with the preferred method of transmission designated by the absent uniformed services voter or overseas voter under subparagraph (C)) voter registration applications and absentee ballot applications requested under subparagraph (A) in accordance with subsection (e); and

"(C) by which the absent uniformed services voter or overseas voter can designate whether the voter prefers that such voter registration application or absentee ballot application be transmitted by mail or electronically."; and

(2) by adding at the end the following new subsection:

"(e) DESIGNATION OF MEANS OF ELECTRONIC COMMUNICATION FOR ABSENT UNIFORMED SERVICES VOTERS AND OVERSEAS VOTERS TO REQUEST AND FOR STATES TO SEND VOTER REGISTRATION APPLICATIONS AND ABSENTEE BALLOT APPLICATIONS, AND FOR OTHER PURPOSES RELATED TO VOTING INFORMATION.—

"(1) IN GENERAL.—Each State shall, in addition to the designation of a single State office under subsection (b), designate not less than 1 means of electronic communication—

"(A) for use by absent uniformed services voters and overseas voters who wish to register to vote or vote in any jurisdiction in the State to request voter registration applications and absentee ballot applications under subsection (a)(6);

"(B) for use by States to send voter registration applications and absentee ballot applications requested under such subsection; and

"(C) for the purpose of providing related voting, balloting, and election information to absent uniformed services voters and overseas voters.

"(2) CLARIFICATION REGARDING PROVISION OF MULTIPLE MEANS OF ELECTRONIC COMMUNICATION.—A State may, in addition to the means of electronic communication so designated, provide multiple means of electronic communication to absent uniformed services voters and overseas voters, including a means of electronic communication for the appropriate jurisdiction of the State.

"(3) INCLUSION OF DESIGNATED MEANS OF ELECTRONIC COMMUNICATION WITH INFORMATIONAL AND INSTRUCTIONAL MATERIALS THAT ACCOMPANY BALLOTING MATERIALS.—Each State shall include a means of electronic communication so designated with all informational and instructional materials that accompany balloting materials sent by the State to absent uniformed services voters and overseas voters.

"(4) AVAILABILITY AND MAINTENANCE OF ONLINE REPOSITORY OF STATE CONTACT INFORMATION.—The Federal Voting Assistance Program of the Department of Defense shall maintain and make available to the public an online repository of State contact information with respect to elections for Federal office, including the single State office designated under subsection (b) and the means of electronic communication designated under paragraph (1), to be used by absent uniformed services voters and overseas voters as a resource to send voter registration applications and absentee ballot applications to the appropriate jurisdiction in the State.

"(5) TRANSMISSION IF NO PREFERENCE INDICATED.—In the case where an absent uniformed services voter or overseas voter does not designate a preference under subsection (a)(6)(C), the State shall transmit the voter registration application or absentee ballot application by any delivery method allowable in accordance with applicable State law, or if there is no applicable State law, by mail.

"(6) SECURITY AND PRIVACY PROTECTIONS.—

"(A) SECURITY PROTECTIONS.—To the extent practicable, States shall ensure that the procedures established under subsection (a)(6) protect the security and integrity of the voter registration and absentee ballot application request processes.

"(B) PRIVACY PROTECTIONS.—To the extent practicable, the procedures established under subsection (a)(6) shall ensure that the privacy of the identity and other personal data of an absent uniformed services voter or overseas voter who requests or is sent a voter registration application or absentee ballot application under such subsection is protected throughout the process of making such request or being sent such application.".

(b) EFFECTIVE DATE.—The amendments made by this section shall apply with respect to the regularly scheduled general election for Federal office held in November 2010 and each succeeding election for Federal office.

SEC. 578. ESTABLISHMENT OF PROCEDURES FOR STATES TO TRANSMIT BLANK ABSENTEE BALLOTS BY MAIL AND ELECTRONICALLY TO ABSENT UNIFORMED SERVICES VOTERS AND OVERSEAS VOTERS.

(a) IN GENERAL.—Section 102 of the Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973ff–1), as amended by section 577, is amended—

(1) in subsection (a)—

(A) in paragraph (5), by striking "and" at the end;

(B) in paragraph (6), by striking the period at the end and inserting "; and"; and

(C) by adding at the end the following new paragraph:

"(7) in addition to any other method of transmitting blank absentee ballots in the State, establish procedures for transmitting by mail and electronically blank absentee ballots to absent uniformed services voters and overseas voters with respect to general, special, primary, and runoff elections for Federal office in accordance with subsection (f).."; and

(2) by adding at the end the following new subsection:

"(f) TRANSMISSION OF BLANK ABSENTEE BALLOTS BY MAIL AND ELECTRONICALLY.—

"(1) IN GENERAL.—Each State shall establish procedures—

"(A) to transmit blank absentee ballots by mail and electronically (in accordance with the preferred method of transmission designated by the absent uniformed services voter or overseas voter under subparagraph (B)) to absent uniformed services voters and overseas voters for an election for Federal office; and

"(B) by which the absent uniformed services voter or overseas voter can designate whether the voter prefers that such blank absentee ballot be transmitted by mail or electronically.

"(2) TRANSMISSION IF NO PREFERENCE INDICATED.—In the case where an absent uniformed services voter or overseas voter does not designate a preference under paragraph (1)(B), the State shall transmit the ballot by any delivery method allowable in accordance with applicable State law, or if there is no applicable State law, by mail.

"(3) SECURITY AND PRIVACY PROTECTIONS.—

"(A) SECURITY PROTECTIONS.—To the extent practicable, States shall ensure that the procedures established under subsection (a)(7) protect the security and integrity of absentee ballots.

"(B) PRIVACY PROTECTIONS.—To the extent practicable, the procedures established under subsection (a)(7) shall ensure that the privacy of the identity and other personal data of an absent uniformed services voter or overseas voter to whom a blank absentee ballot is transmitted under such subsection is protected throughout the process of such transmission.".

(b) EFFECTIVE DATE.—The amendments made by this section shall apply with respect to the regularly scheduled general election for Federal office held in November 2010 and each succeeding election for Federal office.

SEC. 579. ENSURING ABSENT UNIFORMED SERVICES VOTERS AND OVERSEAS VOTERS HAVE TIME TO VOTE.

(a) IN GENERAL.—Section 102 of the Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973ff–1(a)(1)), as amended by sections 577 and 578, is amended—

(1) in subsection (a)—

(A) in paragraph (6), by striking "and" at the end;

(B) in paragraph (7), by striking the period at the end and inserting a semicolon; and

(C) by adding at the end the following new paragraph:

"(8) transmit a validly requested absentee ballot to an absent uniformed services voter or overseas voter—

"(A) except as provided in subsection (g), in the case in which the request is received at least 45 days before an election for Federal office, not later than 45 days before the election; and

"(B) in the case in which the request is received less than 45 days before an election for Federal office—

"(i) in accordance with State law; and

"(ii) if practicable and as determined appropriate by the State, in a manner that expedites the transmission of such absentee ballot.";

(2) by adding at the end the following new subsection:

"(g) HARDSHIP EXEMPTION.—

"(1) IN GENERAL.—If the chief State election official determines that the State is unable to meet the requirement under subsection (a)(8)(A) with respect to an election for Federal office due to an undue hardship described in paragraph (2)(B), the chief State election official shall request that the Presidential designee grant a waiver to the State of the application of such subsection. Such request shall include—

"(A) a recognition that the purpose of such subsection is to allow absent uniformed services voters and overseas voters enough time to vote in an election for Federal office;

"(B) an explanation of the hardship that indicates why the State is unable to transmit absent uniformed services voters and overseas voters an absentee ballot in accordance with such subsection;

"(C) the number of days prior to the election for Federal office that the State requires absentee ballots be transmitted to absent uniformed services voters and overseas voters; and

"(D) a comprehensive plan to ensure that absent uniformed services voters and overseas voters are able to receive absentee ballots which they have requested and submit marked absentee ballots to the appropriate State election official in time to have that ballot counted in the election for Federal office, which includes—

"(i) the steps the State will undertake to ensure that absent uniformed services voters and overseas voters have time to receive, mark, and submit their ballots in time to have those ballots counted in the election;

"(ii) why the plan provides absent uniformed services voters and overseas voters sufficient time to vote as a substitute for the requirements under such subsection; and

"(iii) the underlying factual information which explains how the plan provides such sufficient time to vote as a substitute for such requirements.

"(2) APPROVAL OF WAIVER REQUEST.—After consulting with the Attorney General, the Presidential designee shall approve a waiver request under paragraph (1) if the Presidential designee determines each of the following requirements are met:

"(A) The comprehensive plan under subparagraph (D) of such paragraph provides absent uniformed services voters and overseas voters sufficient time to receive absentee ballots they have requested and submit marked absentee ballots to the appropriate State election official in time to have that ballot counted in the election for Federal office.

"(B) One or more of the following issues creates an undue hardship for the State:

"(i) The State's primary election date prohibits the State from complying with subsection (a)(8)(A).

"(ii) The State has suffered a delay in generating ballots due to a legal contest.

"(iii) The State Constitution prohibits the State from complying with such subsection.

"(3) TIMING OF WAIVER.—

"(A) IN GENERAL.—Except as provided under subparagraph (B), a State that requests a waiver under paragraph (1) shall submit to the Presidential designee the written waiver request not later than 90 days before the election for Federal office with respect to which the request is submitted. The Presidential designee shall approve or deny the waiver request not later than 65 days before such election.

"(B) EXCEPTION.—If a State requests a waiver under paragraph (1) as the result of an undue hardship described in paragraph (2)(B)(ii), the State shall submit to the Presidential designee the written waiver request as soon as practicable. The Presidential designee shall approve or deny the waiver request not later than 5 business days after the date on which the request is received.

"(4) APPLICATION OF WAIVER.—A waiver approved under paragraph (2) shall only apply with respect to the election for Federal office for which the request was submitted. For each subsequent election for Federal office, the Presidential designee shall only approve a waiver if the State has submitted a request under paragraph (1) with respect to such election.".

(b) RUNOFF ELECTIONS.—Section 102(a) of the Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973ff–1(a)), as amended by subsection (a) and sections 577 and 578, is amended—

(1) in paragraph (7), by striking "and" at the end;

(2) in paragraph (8), by striking the period at the end and inserting "; and"; and

(3) by adding at the end the following new paragraph:

"(9) if the State declares or otherwise holds a runoff election for Federal office, establish a written plan that provides absentee ballots are made available to absent uniformed services voters and overseas voters in manner that gives them sufficient time to vote in the runoff election.".

(c) EFFECTIVE DATE.—The amendments made by this section shall apply with respect to the regularly scheduled general election for Federal office held in November 2010 and each succeeding election for Federal office.

SEC. 580. PROCEDURES FOR COLLECTION AND DELIVERY OF MARKED ABSENTEE BALLOTS OF ABSENT OVERSEAS UNIFORMED SERVICES VOTERS.

(a) IN GENERAL.—The Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973ff et seq.) is amended by inserting after section 103 the following new section:

"SEC. 103A. PROCEDURES FOR COLLECTION AND DELIVERY OF MARKED ABSENTEE BALLOTS OF ABSENT OVERSEAS UNIFORMED SERVICES VOTERS.

"(a) ESTABLISHMENT OF PROCEDURES.—The Presidential designee shall establish procedures for collecting marked absentee ballots of absent overseas uniformed services voters in regularly scheduled general elections for Federal office, including absentee ballots prepared by States and the Federal write-in absentee ballot prescribed under section 103, and for delivering such marked absentee ballots to the appropriate election officials.

"(b) DELIVERY TO APPROPRIATE ELECTION OFFICIALS.—

"(1) IN GENERAL.—Under the procedures established under this section, the Presidential designee shall implement procedures that facilitate the delivery of marked absentee ballots of absent overseas uniformed services voters for regularly scheduled general elections for Federal office to the appropriate election officials, in accordance with this section, not later than the date by which an absentee ballot must be received in order to be counted in the election.

"(2) COOPERATION AND COORDINATION WITH THE UNITED STATES POSTAL SERVICE.—The Presidential designee shall carry out this section in cooperation and coordination with the United States Postal Service, and shall provide expedited mail delivery service for all such marked absentee ballots of absent uniformed services voters that are collected on or before the deadline described in paragraph (3) and then transferred to the United States Postal Service.

"(3) DEADLINE DESCRIBED.—

"(A) IN GENERAL.—Except as provided in subparagraph (B), the deadline described in this paragraph is noon (in the location in which the ballot is collected) on the seventh day preceding the date of the regularly scheduled general election for Federal office.

"(B) AUTHORITY TO ESTABLISH ALTERNATIVE DEADLINE FOR CERTAIN LOCATIONS.—If the Presidential designee determines that the deadline described in subparagraph (A) is not sufficient to ensure timely delivery of the ballot under paragraph (1) with respect to a particular location because of remoteness or other factors, the Presidential designee may establish as an alternative deadline for that location the latest date occurring prior to the deadline described in subparagraph (A) which is sufficient to provide timely delivery of the ballot under paragraph (1).

"(4) NO POSTAGE REQUIREMENT.—In accordance with section 3406 of title 39, United States Code, such marked absentee

ballots and other balloting materials shall be carried free of postage.

"(5) DATE OF MAILING.—Such marked absentee ballots shall be postmarked with a record of the date on which the ballot is mailed.

"(c) OUTREACH FOR ABSENT OVERSEAS UNIFORMED SERVICES VOTERS ON PROCEDURES.—The Presidential designee shall take appropriate actions to inform individuals who are anticipated to be absent overseas uniformed services voters in a regularly scheduled general election for Federal office to which this section applies of the procedures for the collection and delivery of marked absentee ballots established pursuant to this section, including the manner in which such voters may utilize such procedures for the submittal of marked absentee ballots pursuant to this section.

"(d) ABSENT OVERSEAS UNIFORMED SERVICES VOTER DEFINED.—In this section, the term 'absent overseas uniformed services voter' means an overseas voter described in section 107(5)(A).

"(e) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Presidential designee such sums as may be necessary to carry out this section.".

(b) CONFORMING AMENDMENT.—Section 101(b) of such Act (42 U.S.C. 1973ff(b)) is amended—

(1) by striking "and" at the end of paragraph (6);

(2) by striking the period at the end of paragraph (7) and inserting "; and"; and

(3) by adding at the end the following new paragraph:

"(8) carry out section 103A with respect to the collection and delivery of marked absentee ballots of absent overseas uniformed services voters in elections for Federal office.".

(c) STATE RESPONSIBILITIES.—Section 102(a) of such Act (42 U.S.C. 1973ff–1(a)), as amended by sections 577, 578, and 579, is amended—

(1) in paragraph (8), by striking "and" at the end;

(2) in paragraph (9), by striking the period at the end and inserting "; and"; and

(3) by adding the following new paragraph:

"(10) carry out section 103A(b)(1) with respect to the processing and acceptance of marked absentee ballots of absent overseas uniformed services voters.".

(d) TRACKING MARKED BALLOTS.—Section 102 of such Act (42 U.S.C. 1973ff–1(a)) is amended by adding at the end the following new subsection:

"(h) TRACKING MARKED BALLOTS.—The chief State election official, in coordination with local election jurisdictions, shall develop a free access system by which an absent uniformed services voter or overseas voter may determine whether the absentee ballot of the absent uniformed services voter or overseas voter has been received by the appropriate State election official.".

(e) PROTECTING VOTER PRIVACY AND SECRECY OF ABSENTEE BALLOTS.—Section 101(b) of the Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973ff(b)), as amended by subsection (b), is amended—

(1) by striking "and" at the end of paragraph (7);

(2) by striking the period at the end of paragraph (8) and inserting "; and"; and

(3) by adding at the end the following new paragraph:

"(9) to the greatest extent practicable, take such actions as may be necessary—

"(A) to ensure that absent uniformed services voters who cast absentee ballots at locations or facilities under the jurisdiction of the Presidential designee are able to do so in a private and independent manner; and

"(B) to protect the privacy of the contents of absentee ballots cast by absentee uniformed services voters and overseas voters while such ballots are in the possession or control of the Presidential designee.".

(f) EFFECTIVE DATE.—The amendments made by this section shall apply with respect to the regularly scheduled general election for Federal office held in November 2010 and each succeeding election for Federal office.

SEC. 581. FEDERAL WRITE-IN ABSENTEE BALLOT.

(a) USE IN GENERAL, SPECIAL, PRIMARY, AND RUNOFF ELECTIONS FOR FEDERAL OFFICE.—

(1) IN GENERAL.—Section 103 of the Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973ff–2) is amended—

(A) in subsection (a), by striking "general elections for Federal office" and inserting "general, special, primary, and runoff elections for Federal office";

(B) in subsection (e), in the matter preceding paragraph (1), by striking "a general election" and inserting "a general, special, primary, or runoff election for Federal office"; and

(C) in subsection (f), by striking "the general election" each place it appears and inserting "the general, special, primary, or runoff election for Federal office".

(2) EFFECTIVE DATE.—The amendments made by this subsection shall take effect on December 31, 2010, and apply with respect to elections for Federal office held on or after such date.

(b) PROMOTION AND EXPANSION OF USE.—Section 103(a) of the Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973ff–2) is amended—

(1) by striking "GENERAL.—The Presidential" and inserting "GENERAL.—

"(1) FEDERAL WRITE-IN ABSENTEE BALLOT.—The Presidential"; and

(2) by adding at the end the following new paragraph:

"(2) PROMOTION AND EXPANSION OF USE OF FEDERAL WRITE-IN ABSENTEE BALLOTS.—

"(A) IN GENERAL.—Not later than December 31, 2011, the Presidential designee shall adopt procedures to promote and expand the use of the Federal write-in absentee ballot as a back-up measure to vote in elections for Federal office.

"(B) USE OF TECHNOLOGY.—Under such procedures, the Presidential designee shall utilize technology to implement a system under which the absent uniformed services voter or overseas voter may—

"(i) enter the address of the voter or other information relevant in the appropriate jurisdiction of the State, and the system will generate a list of all candidates in the election for Federal office in that jurisdiction; and

"(ii) submit the marked Federal write-in absentee ballot by printing the ballot (including complete instructions for submitting the marked Federal write-in absentee ballot to the appropriate State election official and the mailing address of the single State office designated under section 102(b)).

"(C) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Presidential designee such sums as may be necessary to carry out this paragraph.".

SEC. 582. PROHIBITING REFUSAL TO ACCEPT VOTER REGISTRATION AND ABSENTEE BALLOT APPLICATIONS, MARKED ABSENTEE BALLOTS, AND FEDERAL WRITE-IN ABSENTEE BALLOTS FOR FAILURE TO MEET CERTAIN REQUIREMENTS.

(a) VOTER REGISTRATION AND ABSENTEE BALLOT APPLICATIONS.—Section 102 of the Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973ff–1) is amended by adding at the end the following new subsection:

"(i) PROHIBITING REFUSAL TO ACCEPT APPLICATIONS FOR FAILURE TO MEET CERTAIN REQUIREMENTS.—A State shall not refuse to accept and process any otherwise valid voter registration application or absentee ballot application (including the official post card form prescribed under section 101) or marked absentee ballot submitted in any manner by an absent uniformed services voter or overseas voter solely on the basis of the following:

"(1) Notarization requirements.

"(2) Restrictions on paper type, including weight and size.

"(3) Restrictions on envelope type, including weight and size.".

(b) FEDERAL WRITE-IN ABSENTEE BALLOT.—Section 103 of such Act (42 U.S.C. 1973ff–2) is amended—

(1) by redesignating subsection (f) as subsection (g); and

(2) by inserting after subsection (e) the following new subsection:

"(f) PROHIBITING REFUSAL TO ACCEPT BALLOT FOR FAILURE TO MEET CERTAIN REQUIREMENTS.—A State shall not refuse to accept and process any otherwise valid Federal write-in absentee ballot submitted in any manner by an absent uniformed services voter or overseas voter solely on the basis of the following:

"(1) Notarization requirements.

"(2) Restrictions on paper type, including weight and size.

"(3) Restrictions on envelope type, including weight and size.".

(c) EFFECTIVE DATE.—The amendments made by this section shall apply with respect to the regularly scheduled general election for Federal office held in November 2010 and each succeeding election for Federal office.

SEC. 583. FEDERAL VOTING ASSISTANCE PROGRAM IMPROVEMENTS.

(a) FEDERAL VOTING ASSISTANCE PROGRAM IMPROVEMENTS.—

(1) IN GENERAL.—The Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973ff et seq.), as amended by section 580(a), is amended by inserting after section 103A the following new section:

"SEC. 103B. FEDERAL VOTING ASSISTANCE PROGRAM IMPROVEMENTS.

"(a) DUTIES.—The Presidential designee shall carry out the following duties:

"(1) Develop online portals of information to inform absent uniformed services voters regarding voter registration procedures and absentee ballot procedures to be used by such voters with respect to elections for Federal office.

"(2) Establish a program to notify absent uniformed services voters of voter registration information and resources, the availability of the Federal postcard application, and the availability of the Federal write-in absentee ballot on the military Global Network, and shall use the military Global Network to notify absent uniformed services voters of the foregoing 90, 60, and 30 days prior to each election for Federal office.

"(b) CLARIFICATION REGARDING OTHER DUTIES AND OBLIGATIONS.—Nothing in this section shall relieve the Presidential designee of their duties and obligations under any directives or regulations issued by the Department of Defense, including the Department of Defense Directive 1000.04 (or any successor directive or regulation) that is not inconsistent or contradictory to the provisions of this section.

"(c) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Federal Voting Assistance Program of the Department of Defense (or a successor program) such sums as are necessary for purposes of carrying out this section.".

(2) CONFORMING AMENDMENTS.—Section 101 of such Act (42 U.S.C. 1973ff), as amended by section 580, is amended—

(A) in subparagraph (b)—

(i) by striking "and" at the end of paragraph (8);

(ii) by striking the period at the end of paragraph (9) and inserting "; and"; and

(iii) by adding at the end the following new paragraph:

"(10) carry out section 103B with respect to Federal Voting Assistance Program Improvements."; and

(B) by adding at the end the following new subsection:

"(d) AUTHORIZATION OF APPROPRIATIONS FOR CARRYING OUT FEDERAL VOTING ASSISTANCE PROGRAM IMPROVEMENTS.—There are authorized to be appropriated to the Presidential designee such sums as are necessary for purposes of carrying out subsection (b)(10).".

(3) EFFECTIVE DATE.—The amendments made by this subsection shall apply with respect to the regularly scheduled general election for Federal office held in November 2010 and each succeeding election for Federal office.

(b) VOTER REGISTRATION ASSISTANCE FOR ABSENT UNIFORMED SERVICES VOTERS.—

(1) IN GENERAL.—Chapter 80 of title 10, United States Code, is amended by inserting after section 1566 the following new section:

"§ 1566a. Voting assistance: voter assistance offices

"(a) DESIGNATION OF OFFICES ON MILITARY INSTALLATIONS AS VOTER ASSISTANCE OFFICES.—Not later than 180 days after the date of the enactment of the National Defense Authorization Act for Fiscal Year 2010 and under regulations prescribed by the Secretary of Defense under subsection (f), the Secretaries of the military

departments shall designate offices on installations under their jurisdiction to provide absent uniformed services voters, particularly those individuals described in subsection (b), and their family members with the following:

"(1) Information on voter registration procedures and absentee ballot procedures (including the official post card form prescribed under section 101 of the Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973ff).

"(2) Information and assistance, if requested, including access to the Internet where practicable, to register to vote in an election for Federal office.

"(3) Information and assistance, if requested, including access to the Internet where practicable, to update the individual's voter registration information, including instructions for absent uniformed services voters to change their address by submitting the official post card form prescribed under section 101 of the Uniformed and Overseas Citizens Absentee Voting Act to the appropriate State election official.

"(4) Information and assistance, if requested, to request an absentee ballot under the Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973ff et seq.).

"(b) COVERED INDIVIDUALS.—The individuals described in this subsection are absent uniformed services voters who—

"(1) are undergoing a permanent change of duty station;

"(2) are deploying overseas for at least six months;

"(3) are returning from an overseas deployment of at least six months; or

"(4) otherwise request assistance related to voter registration.

"(c) TIMING OF PROVISION OF ASSISTANCE.—The regulations prescribed by the Secretary of Defense under subsection (f) shall ensure, to the maximum extent practicable and consistent with military necessity, that the assistance provided under subsection (a) is provided to a covered individual described in subsection (b)—

"(1) if described in subsection (b)(1), as part of the administrative in-processing of the covered individual upon arrival at the new duty station of the covered individual;

"(2) if described in subsection (b)(2), as part of the administrative out-processing of the covered individual in preparation for deployment from the home duty station of the covered individual;

"(3) if described in subsection (b)(3), as part of the administrative in-processing of the covered individual upon return to the home duty station of the covered individual; or

"(4) if described in subsection (b)(4), at the time the covered individual requests such assistance.

"(d) OUTREACH.—The Secretary of each military department, or the Presidential designee, shall take appropriate actions to inform absent uniformed services voters of the assistance available under subsection (a), including—

"(1) the availability of information and voter registration assistance at offices designated under subsection (a); and

"(2) the time, location, and manner in which an absent uniformed services voter may utilize such assistance.

"(e) AUTHORITY TO DESIGNATE VOTING ASSISTANCE OFFICES AS VOTER REGISTRATION AGENCY ON MILITARY INSTALLATIONS.—The Secretary of Defense may authorize the Secretaries of the

military departments to designate offices on military installations as voter registration agencies under section 7(a)(2) of the National Voter Registration Act of 1993 (42 U.S.C. 1973gg–5(a)(2)) for all purposes of such Act. Any office so designated shall discharge the requirements of this section, under the regulations prescribed by the Secretary of Defense under subsection (f).

"(f) REGULATIONS.—The Secretary of Defense shall prescribe regulations relating to the administration of the requirements of this section. The regulations shall be prescribed before the regularly scheduled general election for Federal office held in November 2010, and shall be implemented for such general election for Federal office and for each succeeding election for Federal office.

"(g) DEFINITIONS.—In this section:

"(1) The term 'absent uniformed services voter' has the meaning given that term in section 107(1) of the Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973ff–6(1)).

"(2) The term 'Federal office' has the meaning given that term in section 107(3) of the Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973ff–6(3)).

"(3) The term 'Presidential designee' means the official designated by the President under section 101(a) of the Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973ff(a)).".

(2) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 80 of such title is amended by inserting after the item relating to section 1566 the following new item:

"1566a. Voting assistance: voter assistance offices.".

SEC. 584. DEVELOPMENT OF STANDARDS FOR REPORTING AND STORING CERTAIN DATA.

(a) IN GENERAL.—Section 101(b) of such Act (42 U.S.C. 1973ff(b)), as amended by sections 580 and 583, is amended—

(1) by striking "and" at the end of paragraph (9);

(2) by striking the period at the end of paragraph (10) and inserting "; and"; and

(3) by adding at the end the following new paragraph:

"(11) working with the Election Assistance Commission and the chief State election official of each State, develop standards—

"(A) for States to report data on the number of absentee ballots transmitted and received under section 102(c) and such other data as the Presidential designee determines appropriate; and

"(B) for the Presidential designee to store the data reported.".

(b) CONFORMING AMENDMENT.—Section 102(a) of such Act (42 U.S.C. 1973ff–1(a)), as amended by sections 577, 578, 579, and 580, is amended—

(1) in paragraph (9), by striking "and" at the end;

(2) in paragraph (10), by striking the period at the end and inserting "; and"; and

(3) by adding at the end the following new paragraph:

"(11) report data on the number of absentee ballots transmitted and received under section 102(c) and such other data

as the Presidential designee determines appropriate in accordance with the standards developed by the Presidential designee under section 101(b)(11).".

(c) EFFECTIVE DATE.—The amendments made by this section shall apply with respect to the regularly scheduled general election for Federal office held in November 2010 and each succeeding election for Federal office.

SEC. 585. REPEAL OF PROVISIONS RELATING TO USE OF SINGLE APPLICATION FOR ALL SUBSEQUENT ELECTIONS.

(a) IN GENERAL.—Subsections (a) through (d) of section 104 of the Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973ff–3) are repealed.

(b) CONFORMING AMENDMENTS.—The Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973ff et seq.) is amended—

(1) in section 101(b)—

(A) in paragraph (2), by striking ", for use by States in accordance with section 104"; and

(B) in paragraph (4), by striking "for use by States in accordance with section 104"; and

(2) in section 104, as amended by subsection (a)—

(A) in the section heading, by striking "**USE OF SINGLE APPLICATION FOR ALL SUBSEQUENT ELECTIONS**" and inserting "**PROHIBITION OF REFUSAL OF APPLICATIONS ON GROUNDS OF EARLY SUBMISSION**"; and

(B) in subsection (e), by striking "(e) PROHIBITION OF REFUSAL OF APPLICATIONS ON GROUNDS OF EARLY SUBMISSION.—".

SEC. 586. REPORTING REQUIREMENTS.

The Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973ff et seq.) is amended by inserting after section 105 the following new section:

"SEC. 105A. REPORTING REQUIREMENTS.

"(a) REPORT ON STATUS OF IMPLEMENTATION AND ASSESSMENT OF PROGRAMS.—Not later than 180 days after the date of the enactment of the Military and Overseas Voter Empowerment Act, the Presidential designee shall submit to the relevant committees of Congress a report containing the following information:

"(1) The status of the implementation of the procedures established for the collection and delivery of marked absentee ballots of absent overseas uniformed services voters under section 103A, and a detailed description of the specific steps taken towards such implementation for the regularly scheduled general election for Federal office held in November 2010.

"(2) An assessment of the effectiveness of the Voting Assistance Officer Program of the Department of Defense, which shall include the following:

"(A) A thorough and complete assessment of whether the Program, as configured and implemented as of such date of enactment, is effectively assisting absent uniformed services voters in exercising their right to vote.

"(B) An inventory and explanation of any areas of voter assistance in which the Program has failed to accomplish its stated objectives and effectively assist absent uniformed services voters in exercising their right to vote.

"(C) As necessary, a detailed plan for the implementation of any new program to replace or supplement voter assistance activities required to be performed under this Act.

"(3) A detailed description of the specific steps taken towards the implementation of voter registration assistance for absent uniformed services voters under section 1566a of title 10, United States Code.

"(b) ANNUAL REPORT ON EFFECTIVENESS OF ACTIVITIES AND UTILIZATION OF CERTAIN PROCEDURES.—Not later than March 31 of each year, the Presidential designee shall transmit to the President and to the relevant committees of Congress a report containing the following information:

"(1) An assessment of the effectiveness of activities carried out under section 103B, including the activities and actions of the Federal Voting Assistance Program of the Department of Defense, a separate assessment of voter registration and participation by absent uniformed services voters, a separate assessment of voter registration and participation by overseas voters who are not members of the uniformed services, and a description of the cooperation between States and the Federal Government in carrying out such section.

"(2) A description of the utilization of voter registration assistance under section 1566a of title 10, United States Code, which shall include the following:

"(A) A description of the specific programs implemented by each military department of the Armed Forces pursuant to such section.

"(B) The number of absent uniformed services voters who utilized voter registration assistance provided under such section.

"(3) In the case of a report submitted under this subsection in the year following a year in which a regularly scheduled general election for Federal office is held, a description of the utilization of the procedures for the collection and delivery of marked absentee ballots established pursuant to section 103A, which shall include the number of marked absentee ballots collected and delivered under such procedures and the number of such ballots which were not delivered by the time of the closing of the polls on the date of the election (and the reasons such ballots were not so delivered).

"(c) DEFINITIONS.—In this section:

"(1) ABSENT OVERSEAS UNIFORMED SERVICES VOTER.—The term 'absent overseas uniformed services voter' has the meaning given such term in section 103A(d).

"(2) PRESIDENTIAL DESIGNEE.—The term 'Presidential designee' means the Presidential designee under section 101(a).

"(3) RELEVANT COMMITTEES OF CONGRESS DEFINED.—The term 'relevant committees of Congress' means—

"(A) the Committees on Appropriations, Armed Services, and Rules and Administration of the Senate; and

"(B) the Committees on Appropriations, Armed Services, and House Administration of the House of Representatives.".

SEC. 587. ANNUAL REPORT ON ENFORCEMENT.

Section 105 of the Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973f–4) is amended—

(1) by striking "The Attorney" and inserting "(a) IN GENERAL.—The Attorney"; and

(2) by adding at the end the following new subsection: "(b) REPORT TO CONGRESS.—Not later than December 31 of each year, the Attorney General shall submit to Congress an annual report on any civil action brought under subsection (a) during the preceding year.".

SEC. 588. REQUIREMENTS PAYMENTS.

(a) USE OF FUNDS.—Section 251(b) of the Help America Vote Act of 2002 (42 U.S.C. 15401(b)) is amended—

(1) in paragraph (1), by striking "paragraph (2)" and inserting "paragraphs (2) and (3)"; and

(2) by adding at the end the following new paragraph: "(3) ACTIVITIES UNDER UNIFORMED AND OVERSEAS CITIZENS ABSENTEE VOTING ACT.—A State shall use a requirements payment made using funds appropriated pursuant to the authorization under section 257(a)(4) only to meet the requirements under the Uniformed and Overseas Citizens Absentee Voting Act imposed as a result of the provisions of and amendments made by the Military and Overseas Voter Empowerment Act.".

(b) CONDITIONS FOR RECEIPT OF FUNDS.—

(1) INCLUSION OF COMPLIANCE IN STATE PLAN.—

(A) IN GENERAL.—Section 254(a) of the Help America Vote Act of 2002 (42 U.S.C. 15404(a)) is amended by adding at the end the following new paragraph:

"(14) How the State will comply with the provisions and requirements of and amendments made by the Military and Overseas Voter Empowerment Act.".

(B) CONFORMING AMENDMENT.—Section 253(b)(1)(A) of such Act (42 U.S.C. 15403(b)(1)(A)) is amended by striking "section 254" and inserting "section 254(a) (or, for purposes of determining the eligibility of a State to receive a requirements payment appropriated pursuant to the authorization provided under section 257(a)(4), contains the element described in paragraph (14) of such section)".

(2) WAIVER OF PLAN FOR APPLICATION OF ADMINISTRATIVE COMPLAINT PROCEDURES.—Section 253(b)(2) of such Act (42 U.S.C. 15403(b)(2)) is amended—

(A) by striking "(2) The State" and inserting "(2)(A) Subject to subparagraph (B), the State"; and

(B) by adding at the end the following new subparagraph:

"(B) Subparagraph (A) shall not apply for purposes of determining the eligibility of a State to receive a requirements payment appropriated pursuant to the authorization provided under section 257(a)(4).".

(3) SPECIAL RULE FOR PROVISION OF 5 PERCENT MATCH.—Section 253(b)(5) of such Act (42 U.S.C. 15403(b)(5)) is amended—

(A) by striking "(5) The State" and inserting "(5)(A) Subject to subparagraph (B), the State"; and

(B) by adding at the end the following new subparagraph:

"(B) Subparagraph (A) shall not apply for purposes of determining the eligibility of a State to receive a requirements payment appropriated pursuant to the authorization provided under section 257(a)(4) for fiscal year 2010, except that if the State does not appropriate funds in accordance with subparagraph (A) prior to the last day of fiscal year 2011, the State shall repay to the Commission the requirements payment which is appropriated pursuant to such authorization.".

(c) AUTHORIZATION.—Section 257(a) of the Help America Vote Act of 2002 (42 U.S.C. 15407(a)) is amended by adding at the end the following new paragraph:

"(4) For fiscal year 2010 and subsequent fiscal years, such sums as are necessary for purposes of making requirements payments to States to carry out the activities described in section 251(b)(3).".

SEC. 589. TECHNOLOGY PILOT PROGRAM.

(a) DEFINITIONS.—In this section:

(1) ABSENT UNIFORMED SERVICES VOTER.—The term "absent uniformed services voter" has the meaning given such term in section 107(a) of the Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973ff et seq.).

(2) OVERSEAS VOTER.—The term "overseas voter" has the meaning given such term in section 107(5) of such Act.

(3) PRESIDENTIAL DESIGNEE.—The term "Presidential designee" means the individual designated under section 101(a) of such Act.

(b) ESTABLISHMENT.—

(1) IN GENERAL.—The Presidential designee may establish 1 or more pilot programs under which the feasibility of new election technology is tested for the benefit of absent uniformed services voters and overseas voters claiming rights under the Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973ff et seq.).

(2) DESIGN AND CONDUCT.—The design and conduct of a pilot program established under this subsection—

(A) shall be at the discretion of the Presidential designee; and

(B) shall not conflict with or substitute for existing laws, regulations, or procedures with respect to the participation of absent uniformed services voters and military voters in elections for Federal office.

(c) CONSIDERATIONS.—In conducting a pilot program established under subsection (b), the Presidential designee may consider the following issues:

(1) The transmission of electronic voting material across military networks.

(2) Virtual private networks, cryptographic voting systems, centrally controlled voting stations, and other information security techniques.

(3) The transmission of ballot representations and scanned pictures in a secure manner.

(4) Capturing, retaining, and comparing electronic and physical ballot representations.

(5) Utilization of voting stations at military bases.

(6) Document delivery and upload systems.

(7) The functional effectiveness of the application or adoption of the pilot program to operational environments, taking into account environmental and logistical obstacles and State procedures.

(d) REPORTS.—The Presidential designee shall submit to Congress reports on the progress and outcomes of any pilot program conducted under this subsection, together with recommendations—

(1) for the conduct of additional pilot programs under this section; and

(2) for such legislation and administrative action as the Presidential designee determines appropriate.

(e) TECHNICAL ASSISTANCE.—

(1) IN GENERAL.—The Election Assistance Commission and the National Institute of Standards and Technology shall provide the Presidential designee with best practices or standards in accordance with electronic absentee voting guidelines established under the first sentence of section 1604(a)(2) of the National Defense Authorization Act for Fiscal Year 2002 (Public Law 107–107; 115 Stat. 1277; 42 U.S.C. 1977ff note), as amended by section 567 of the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005 (Public Law 108–375; 118 Stat. 1919) to support the pilot program or programs.

(2) REPORT.—In the case in which the Election Assistance Commission has not established electronic absentee voting guidelines under such section 1604(a)(2), as so amended, by not later than 180 days after enactment of this Act, the Election Assistance Commission shall submit to the relevant committees of Congress a report containing the following information:

(A) The reasons such guidelines have not been established as of such date.

(B) A detailed timeline for the establishment of such guidelines.

(C) A detailed explanation of the Commission's actions in establishing such guidelines since the date of enactment of the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005 (Public Law 108–375; 118 Stat. 1919).

(3) RELEVANT COMMITTEES OF CONGRESS DEFINED.—In this subsection, the term "relevant committees of Congress" means—

(A) the Committees on Appropriations, Armed Services, and Rules and Administration of the Senate; and

(B) the Committees on Appropriations, Armed Services, and House Administration of the House of Representatives.

(f) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated such sums as are necessary to carry out this section.

Subtitle I—Other Matters

SEC. 591. CLARIFICATION OF PERFORMANCE POLICIES FOR MILITARY MUSICAL UNITS AND MUSICIANS.

(a) CLARIFICATION.—Section 974 of title 10, United States Code, is amended to read as follows:

Attachment B – Relevant Sections of the 2002 National Defense Authorization Act

"(b) In this section, the term 'State' includes a territory or possession of the United States, a political subdivision of a State, territory, or possession, and the District of Columbia.".

SEC. 1604. ELECTRONIC VOTING DEMONSTRATION PROJECT.

42 USC 1973ff note.

(a) ESTABLISHMENT OF DEMONSTRATION PROJECT.—

(1) IN GENERAL.—Subject to paragraph (2), the Secretary of Defense shall carry out a demonstration project under which absent uniformed services voters are permitted to cast ballots in the regularly scheduled general election for Federal office for November 2002 through an electronic voting system. The project shall be carried out with participation of sufficient numbers of absent uniformed services voters so that the results are statistically relevant.

(2) AUTHORITY TO DELAY IMPLEMENTATION.—If the Secretary of Defense determines that the implementation of the demonstration project under paragraph (1) with respect to the regularly scheduled general election for Federal office for November 2002 may adversely affect the national security of the United States, the Secretary may delay the implementation of such demonstration project until the regularly scheduled general election for Federal office for November 2004. The Secretary shall notify the Committee on Armed Services and the Committee on Rules and Administration of the Senate and the Committee on Armed Services and the Committee on House Administration of the House of Representatives of any decision to delay implementation of the demonstration project.

(b) COORDINATION WITH STATE ELECTION OFFICIALS.—The Secretary shall carry out the demonstration project under this section through cooperative agreements with State election officials of States that agree to participate in the project.

(c) REPORT TO CONGRESS.—Not later than June 1 of the year following the year in which the demonstration project is conducted under this section, the Secretary of Defense shall submit to Congress a report analyzing the demonstration project. The Secretary shall include in the report any recommendations the Secretary considers appropriate for continuing the project on an expanded basis for absent uniformed services voters during the next regularly scheduled general election for Federal office.

Deadline.

(d) DEFINITIONS.—In this section:

(1) ABSENT UNIFORMED SERVICES VOTER.—The term "absent uniformed services voter" has the meaning given that term in section 107(1) of the Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973ff–6(1)).

(2) STATE.—The term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, Guam, the Virgin Islands, and American Samoa.

SEC. 1605. GOVERNORS' REPORTS ON IMPLEMENTATION OF RECOMMENDATIONS FOR CHANGES IN STATE LAW MADE UNDER FEDERAL VOTING ASSISTANCE PROGRAM.

42 USC 1973ff note.

(a) REPORTS.—(1) Whenever a State receives a uniformed services voting assistance legislative recommendation from the Secretary of Defense, acting as the Presidential designee, the chief executive authority of that State shall, not later than 90 days after receipt of that recommendation, provide a report on the status of implementation of that recommendation by that State.

Attachment C – Relevant Sections of the 2005 National Defense Authorization Act

Subtitle I—Military Voting

SEC. 566. FEDERAL WRITE-IN BALLOTS FOR ABSENTEE MILITARY VOTERS LOCATED IN THE UNITED STATES.

(a) DUTIES OF PRESIDENTIAL DESIGNEE.—Section 101(b)(3) of the Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973ff(b)(3)) is amended by striking "overseas voters" and inserting "absent uniformed services voters and overseas voters".

(b) STATE RESPONSIBILITIES.—Section 102(a)(3) of such Act (42 U.S.C. 1973ff–1(a)(3)) is amended by striking "overseas voters" and inserting "absent uniformed services voters and overseas voters".

(c) FEDERAL WRITE-IN ABSENTEE BALLOT.—Section 103 of such Act (42 U.S.C. 1973ff–2) is amended—

(1) in subsection (a), by striking "overseas voters" and inserting "absent uniformed services voters and overseas voters";

(2) in subsection (b), by striking the second sentence and inserting the following new sentence: "A Federal write-in absentee ballot of an absent uniformed services voter or overseas voter shall not be counted—

"(1) in the case of a ballot submitted by an overseas voter who is not an absent uniformed services voter, if the ballot is submitted from any location in the United States;

"(2) if the application of the absent uniformed services voter or overseas voter for a State absentee ballot is received by the appropriate State election official after the later of—

"(A) the deadline of the State for receipt of such application; or

"(B) the date that is 30 days before the general election; or

"(3) if a State absentee ballot of the absent uniformed services voter or overseas voter is received by the appropriate State election official not later than the deadline for receipt of the State absentee ballot under State law.";

(3) in subsection (c)(1), by striking "overseas voter" and inserting "absent uniformed services voter or overseas voter";

(4) in subsection (d), by striking "overseas voter" both places it appears and inserting "absent uniformed services voter or overseas voter"; and

(5) in subsection (e)(2), by striking "overseas voters" and inserting "absent uniformed services voters and overseas voters".

(d) CONFORMING AMENDMENTS.—(1) The heading of section 103 of such Act is amended to read as follows:

"SEC. 103. FEDERAL WRITE-IN ABSENTEE BALLOT IN GENERAL ELECTIONS FOR FEDERAL OFFICE FOR ABSENT UNIFORMED SERVICES VOTERS AND OVERSEAS VOTERS.".

(2) The subsection caption for subsection (d) of such section is amended by striking "OVERSEAS VOTER" and inserting "ABSENT UNIFORMED SERVICES VOTER OR OVERSEAS VOTER".

SEC. 567. REPEAL OF REQUIREMENT TO CONDUCT ELECTRONIC VOTING DEMONSTRATION PROJECT FOR THE FEDERAL ELECTION TO BE HELD IN NOVEMBER 2004.

The first sentence of section 1604(a)(2) of the National Defense Authorization Act for Fiscal Year 2002 (Public Law 107–107; 115

Stat. 1277; 42 U.S.C. 1977ff note) is amended by striking "until the regularly scheduled general election for Federal office for November 2004" and inserting the following: "until the first regularly scheduled general election for Federal office which occurs after the Election Assistance Commission notifies the Secretary that the Commission has established electronic absentee voting guidelines and certifies that it will assist the Secretary in carrying out the project".

SEC. 568. REPORTS ON OPERATION OF FEDERAL VOTING ASSISTANCE PROGRAM AND MILITARY POSTAL SYSTEM.

(a) REPORTS ON PROGRAM AND SYSTEM.—(1) Not later than 60 days after the date of the enactment of this Act, the Secretary of Defense shall submit to Congress a report on the actions that the Secretary has taken to ensure that the Federal Voting Assistance Program carried out under the Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973ff et seq.) functions effectively to support absentee voting by members of the Armed Forces deployed outside the United States in support of Operation Iraqi Freedom, Operation Enduring Freedom, and all other contingency operations.

(2) Not later than 60 days after the date of the submission of the report required by paragraph (1), the Secretary of Defense shall submit to Congress a report on the actions that the Secretary has taken to ensure that the military postal system functions effectively to support the morale of members referred to in such paragraph and their ability to vote by absentee ballot.

(b) REPORT ON IMPLEMENTATION OF POSTAL SYSTEM IMPROVEMENTS.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Defense shall submit to Congress a report specifying—

(1) the actions taken to implement the recommendations of the Military Postal Service Agency Task Force, dated 28 August 2000; and

(2) in the case of each recommendation not implemented or not fully implemented as of the date of the submission of the report, the reasons for not implementing or not fully implementing the recommendation, as the case may be.

Subtitle J—Military Justice Matters

SEC. 571. REVIEW ON HOW SEXUAL OFFENSES ARE COVERED BY UNIFORM CODE OF MILITARY JUSTICE.

(a) REVIEW REQUIRED.—The Secretary of Defense shall review the Uniform Code of Military Justice and the Manual for Courts-Martial with the objective of determining what changes are required to improve the ability of the military justice system to address issues relating to sexual assault and to conform the Uniform Code of Military Justice and the Manual for Courts-Martial more closely to other Federal laws and regulations that address such issues.

(b) REPORT.—Not later than March 1, 2005, the Secretary shall submit to the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives a report on the review carried out under subsection (a). The report shall include the recommendations of the Secretary for revisions

Attachment D – EAC's Draft Voting System Pilot Program Testing and Certification Manual (out for public comment)

United States Election Assistance Commission

1201 New York Avenue. N.W.
Ste.300
Washington, DC 20005
202-566-3100

Voting System Pilot Program Testing & Certification Manual

Version 1.0 - Effective XXX 1, 2010 ***www.eac.gov***

OMB Control Number xxxx-xxxx

The reporting requirements in this manual have been approved under the Paperwork Reduction Act of 1995, Office of Management and Budget Control (OMB) Number xxxx-xxxx, expiring DATE. Persons are not required to respond to this collection of information unless it displays a currently valid OMB number. Information gathered pursuant to this document and its forms will be used solely to administer the EAC Pilot Program Testing Program. This program is voluntary. Individuals who wish to participate in the program, however, must meet its requirements. The estimated total annual hourly burden on the voting system manufacturing industry and election officials is XXX hours. This estimate includes the time required for reviewing the instructions, gathering information, and completing the prescribed forms. Send comments regarding this burden estimate or any other aspect of this collection, including suggestions for reducing this burden, to the U.S. Election Assistance Commission, Voting System Testing and Certification Program, Office of the Program Director, 1201 New York Avenue, NW, Suite 300, Washington, D.C. 20005.

Table of Contents

1. Introduction 1

2. Manufacturer Registration 10

3. When Voting Systems Intended for Use in Pilot Programs Must Be Submitted for Testing and Certification 16

4. Certification Testing, Technical Review and Grant of Certification for Pilot Voting Systems 18

5. Denial of Certification 29

6. Pilot Program Monitoring and Reporting 33

7. Requests for Interpretations 39

8. Release of Certification Program Information 43

Appendix A 48

Appendix B 49

Appendix C 50

1. Introduction

1.1. Background. In late 2002, Congress passed the Help America Vote Act of 2002 (HAVA). HAVA created the U.S. Election Assistance Commission (EAC) and assigned to the EAC the responsibility for both setting voting system standards and providing for the testing and certification of voting systems. In response to this HAVA requirement, the EAC developed the Voting System Testing and Certification Program (Certification Program). This manual, governing participation in Pilot Program testing and certification programs is a natural adjunct to the full EAC Testing and Certification Program.

1.2. Authority. HAVA requires that the EAC certify and decertify voting systems. Section 231(a)(1) of HAVA specifically requires the EAC to "… provide for the testing, certification, decertification and recertification of voting system hardware and software by accredited laboratories." The EAC has the sole authority to grant certification or withdraw certification at the Federal level, including the authority to grant, maintain, extend, suspend, and withdraw the right to retain or use any certificates, marks, or other indicators of certification.

1.3. Scope. This Manual provides the procedural requirements of the EAC Testing and Certification Program for voting systems used in pilot projects. Although participation in the program is voluntary, adherence to the program's procedural requirements is mandatory for participants.

1.4. Purpose. The primary purpose of the EAC Pilot Program Certification Manual is to provide clear procedures to Manufacturers for the testing and certification of voting systems to be used in pilot election projects. The program also recognizes that the Federal certification framework should encourage the voting systems industry to pursue technological innovation and experimentation in relation to the design of voting systems and the methods of providing a better and more secure voting experience for United States citizens. This Manual provides a clear and transparent process for the testing, certification, and evaluation of voting systems used for these pilot programs.

1.5. Manual. This Manual is a comprehensive presentation of the EAC Pilot Testing and Certification Program. It is intended to establish all of the program's administrative requirements.

1.5.1. Contents. The contents of the Manual serve as an overview of the program itself. The Manual contains the following chapters:

1.5.1.1. *Manufacturer Registration*. Under the program, a Manufacturer is required to register with the EAC prior to participation in pilot programs requiring Federal certification. This registration provides the EAC with needed information and requires the Manufacturer to agree to the requirements of the Pilot Certification Program. This chapter sets out the requirements and procedures for registration.

OMB Control Number xxxx-xxxx

1.5.1.2. *When Voting Systems Intended for Use in Pilot Programs Must Be Submitted for Testing and Certification*. All pilot voting systems must be submitted consistent with this Manual before they may receive a certification from the EAC. This chapter discusses the various circumstances that require submission to obtain a certification.

1.5.1.3. *Certification Testing, Technical Review and grant of Certification for Pilot Systems.* This chapter discusses the procedural requirements for submitting a pilot voting system to the EAC for testing and review. The testing and review process requires an application, employment of an EAC accredited testing laboratory, and technical analysis of the laboratory test plan and test report by the EAC. The result of this process is a Decision on Certification by the Decision Authority.

1.5.1.4. *Denial of Certification*. If a decision to deny certification is made, the Manufacturer has certain rights and responsibilities under the program. This chapter contains procedures for opportunity to cure defects, and appeal.

1.5.1.5. *Pilot Program Monitoring and Reporting*. This chapter provides the EAC with two primary and one secondary tool for assessing the level of compliance to requirements and performance to mission (pilot) objectives of pilot program voting systems. The primary tools are (1) manufacturer declaration of conformity audits and (2) mandatory post election reporting by manufacturers. The secondary tool for monitoring the effectiveness of the program and of the pilot system consists of voluntary pilot program monitoring and reporting by State and local election jurisdiction participating in pilot programs.

1.5.1.6. *Requests for Interpretations*. An Interpretation is a means by which a registered Manufacturer or Voting System Test Laboratory (VSTL) may seek clarification on a specific Voting System standard or testable requirement. This chapter outlines the policy, requirements, and procedures for requesting an Interpretation.

1.5.1.7. *Release of Certification Program Information*. Federal law protects certain types of information individuals provided the government from release. This chapter outlines the program's policies, sets procedures, and discusses responsibilities associated with the public release of potential protected commercial information.

1.5.2. Maintenance and Revision. The Manual will be reviewed periodically and updated to meet the needs of the EAC, Manufacturers, VSTLs, election officials, and public policy. The EAC is responsible for revising this document. All revisions will be made consistent with Federal law. Substantive input from stakeholders and the public will be

sought whenever possible, at the discretion of the agency. Changes in policy requiring immediate implementation will be noticed via policy memoranda and will be issued to each registered Manufacturer. Changes, addendums, or updated versions will also be posted to the EAC Web site at www.eac.gov.

1.6. Program Methodology. EAC's Pilot Testing and Certification Program is but one part of the overall conformity assessment process that includes the EAC Voting System Testing and Certification Program as well as companion testing efforts at the State and local levels.

1.6.1. Federal and State Roles. The process to ensure that voting equipment meets the technical requirements is a distributed, cooperative effort of Federal, State, and local officials in the United States. Working with voting equipment Manufacturers, these officials each have unique responsibility for ensuring that the equipment a voter uses on Election Day meets specific requirements.

1.6.1.1. The EAC Program has primary responsibility for ensuring that voting systems submitted under this program meet Federal standards established for voting systems.

1.6.1.2. State officials have responsibility for testing voting systems to ensure that they will support the specific requirements of each individual State. States may use EAC VSTLs to perform testing of voting systems to unique State requirements while the systems are being tested to Federal standards. The EAC will not, however, certify voting systems to State requirements.

1.6.1.3. State or local officials are responsible for making the final purchase choice. They are responsible for deciding which system offers the best fit and total value for their specific State or local jurisdiction.

1.6.1.4. State or local officials are also responsible for acceptance testing to ensure that the equipment delivered is identical to the equipment certified on the Federal and State levels, is fully operational, and meets the contractual requirements of the purchase.

1.6.1.5. State or local officials should perform pre-election logic and accuracy testing to confirm that equipment is operating properly and is unmodified from its certified state.

1.7. Program Personnel. All EAC personnel and contractors associated with this program will be held to the highest ethical standards. All agents of the EAC involved in the Certification Program will be subject to conflict-of-interest reporting and review, consistent with Federal law and regulation.

1.8. Program Records. The EAC Program Director is responsible for maintaining accurate records to demonstrate that the pilot program testing and certification procedures have been effectively fulfilled and to ensure the traceability, repeatability, and reproducibility of testing and test

report review. All records will be maintained, managed, secured, stored, archived, and disposed of in accordance with Federal law, Federal regulations, and procedures of the EAC.

1.9. Submission of Documents. Any documents submitted pursuant to the requirements of this Manual shall be submitted:

1.9.1. If sent electronically, via secure e-mail or physical delivery of a compact disk, unless otherwise specified.

1.9.2. In a Microsoft Word or Adobe PDF file, formatted to protect the document from alteration.

1.9.3. With a proper signature when required by this Manual. Documents that require an authorized signature may be signed with an electronic representation or image of the signature of an authorized management representative and must meet any and all subsequent requirements established by the Program Director regarding security.

1.9.4. If sent via physical delivery, by Certified Mail™ (or similar means that allows tracking) to the following address:

Testing and Certification Program Director
U.S. Election Assistance Commission
1201 New York Avenue, NW, Suite 300
Washington, D.C. 20005

1.10. Receipt of Documents—Manufacturer. For purposes of this Manual, a document, notice, or other communication is considered received by a Manufacturer upon one of the following:

1.10.1. The actual, documented date the correspondence was received (either electronically or physically) at the Manufacturer's place of business, or

1.10.2. If no documentation of the actual delivery date exists, the date of constructive receipt of the communication. For electronic correspondence, documents will be constructively received the day after the date sent. For mail correspondence, the document will be constructively received 3 days after the date sent.

1.10.3. The term "receipt" shall mean the date a document or correspondence arrives (either electronically or physically) at the Manufacturer's place of business. Arrival does not require that an agent of the Manufacturer open, read, or review the correspondence.

1.11. Receipt of Documents—EAC. For purposes of this Manual, a document, notice, or other communication is considered received by the EAC upon its physical or electronic arrival at the agency. All documents received by the agency will be physically or electronically date stamped. This stamp shall serve as the date of receipt. Documents received after the regular business day (5:00 PM Eastern Standard Time), will be treated as if received on the next business day.

1.12. EAC Response Timeframes. In recognition of the unique challenges facing Manufacturers and election jurisdictions as they work to meet the requirements imposed by this program, and by running an election using a pilot voting system, the EAC will respond in an expedited manner for each of the program areas outlined in this Manual. Specific response timeframes are noted in each section of the Manual.

1.13. Records Retention—Manufacturers. The Manufacturer is responsible for ensuring that all documents submitted to the EAC or that otherwise serve as the basis for the certification of a voting system are retained. A copy of all such records shall be retained as long as a voting system is offered for sale or supported by a Manufacturer and for 5 years thereafter.

1.14. Record Retention—EAC. The EAC shall retain all records associated with the certification of a voting system as long as such system is fielded in a State or local election jurisdiction for use in Federal elections. The records shall otherwise be retained or disposed of consistent with Federal statutes and regulations.

1.15. Publication and Release of Documents. The EAC will release documents consistent with the requirements of Federal law. It is EAC policy to make the certification process as open and public as possible. Any documents (or portions thereof) submitted under this program will be made available to the public unless specifically protected from release by law. The primary means for making this information available is through the EAC Web site.

OMB Control Number xxxx-xxxx

1.16. Definitions. For purposes of this Manual, the terms listed below have the following definitions.

Anomaly. An anomaly is any irregular or inconsistent action or response from the voting system or system component resulting in some disruption to the election process.

Appeal. A formal process by which the EAC is petitioned to reconsider an Agency Decision.

Appeal Authority. The individual or individuals appointed to serve as the determination authority on appeal.

Audit. An independent, systematic and documented process for obtaining evidence and evaluating it objectively to determine if the auditing criteria have been fulfilled by the voting system manufacturer.

Audit Criteria. A set of policies, procedures and requirements used as a reference for audit evidence.

Audit Evidence. Verifiable records, statements or other information relevant to the audit criteria.

Build Environment. The disk or other media that holds the source code, compiler, linker, integrated development environments (IDE), and/or other necessary files for the compilation and on which the compiler will store the resulting executable code.

Certificate of Conformance. The certificate issued by the EAC when a system has been found to meet the requirements of the VVSG. The document conveys certification of a system.

Commission. The U.S. Election Assistance Commission, as an agency.

Commissioners. The serving commissioners of the U.S. Election Assistance Commission.

Component. A discrete and identifiable element of hardware or software within a larger voting system.

Compiler. A computer program that translates programs expressed in a high-level language into machine language equivalents.

Contributing Cause. A reason that an anomaly occurred. A contributing cause indirectly affects that outcome or occurrence but on its own may not create the problem.

Corrective Action. An action taken to eliminate the root cause of an existing anomaly in order to prevent future occurrences of the anomaly.

OMB Control Number xxxx-xxxx

Days. Calendar days, unless otherwise noted. When counting days, for the purpose of submitting or receiving a document, the count shall begin on the first full calendar day after the date the document was received.

Declaration of Conformance. Procedure by which the manufacturer of a pilot voting system gives written assurance that their product, process and service conforms to specified requirements.

Disk Image. An exact copy of the entire contents of a computer disk.

Election Official. A State or local government employee who has as one of his or her primary duties the management or administration of a Federal election.

Federal Election. Any primary, general, runoff, or special Election in which a candidate for Federal office (President, Senator, or Representative) appears on the ballot.

Fielded Voting System. A voting system purchased or leased by a State or local government that is being use in a Federal election.

File Signature. A signature of a file or set of files produced using a HASH algorithm. A file signature, sometimes called a HASH value, creates a value that is computationally infeasible of being produced by two similar but different files. File signatures are used to verify that files are unmodified from their original versions.

HASH Algorithm. An algorithm that maps a bit string of arbitrary length to a shorter, fixed-length bit string. (A HASH uniquely identifies a file similar to the way a fingerprint identifies an individual. Likewise, as an individual cannot be recreated from his or her fingerprint, a file cannot be recreated from a HASH. The HASH algorithm used primarily in the NIST (National Software Reference Library) and this program is the Secure HASH Algorithm (SHA-1) specified in Federal Information Processing Standard (FIPS) 180-1.)

Installation Device. A device containing program files, software, and installation instructions for installing an application (program) onto a computer. Examples of such devices include installation disks, flash memory cards, and PCMCIA cards.

Integration Testing. The end-to-end testing of a full system configured for use in an election to assure that all legitimate configurations meet applicable standards.

Linker. A computer program that takes one or more objects generated by compilers and assembles them into a single executable program.

Manufacturer. The entity with ownership and control over a voting system submitted for certification.

Mark of Conformance. A uniform notice permanently posted on a voting system that signifies that it has been certified by the EAC.

Memorandum for the Record. A written statement drafted to document an event or finding, without a specific addressee other than the pertinent file.

Proprietary Information. Commercial information or trade secrets protected from release under the Freedom of Information Act (FOIA) and the Trade Secrets Act.

Root Cause. The fundamental reason an anomaly occurred.

Root Cause Analysis. A systematic investigation of the circumstances and factors leading to an anomaly for purposes of finding the fundamental reason for that anomaly.

System Identification Tools. Tools created by a Manufacturer of voting systems that allow elections officials to verify that the hardware and software of systems purchased are identical to the systems certified by the EAC.

Technical Reviewers. Technical experts in the areas of voting system technology and conformity assessment appointed by the EAC to provide expert guidance.

Testing and Certification Decision Authority. The EAC Executive Director or Acting Executive Director.

Testing and Certification Program Director. The individual appointed by the EAC Executive Director to administer and manage the Testing and Certification Program.

Trusted Build. A witnessed software build where source code is converted to machine-readable binary instructions (executable code) in a manner providing security measures that help ensure that the executable code is a verifiable and faithful representation of the source code.

Voting System. The total combination of mechanical, electromechanical, and electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment) that is used to define ballots, cast and count votes, report or display election results, connect the voting system to the voter registration system, and maintain and produce any audit trail information.

Voting System Pilot Program. While there is no general statutory definition of “pilot program,” all such programs exhibit certain common characteristics: experimental purpose and limited duration and scope. The accepted definition of ‘pilot program’ means a limited roll out of a new system in order to test it under real world conditions, prior to use by an entire organization. For voting systems, the purpose of any pilot program is to gain first hand experience with the new technology implemented for the pilot program election, and to evaluate the system and its benefits to domestic or overseas voters.

Voting System Standards. Voting System Standards have been published twice: once in 1990 and again in 2002 by the FEC. The Help America Vote Act made the 2002 Voting System

Standards EAC guidance. All new voting system standards are issued by the EAC as Voluntary Voting System Guidelines.

Voting System Test Laboratories. Laboratories accredited by the EAC to test voting systems to EAC approved voting system standards. Each Voting System Test Laboratory (VSTL) must be accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and recommended by the National Institute of Standards Technology (NIST) before it may receive an EAC accreditation. NVLAP provides third party accreditation to testing and calibration laboratories. NVLAP is in full conformance with the standards of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), including ISO/IEC Guide 17025 and 17011.

Voluntary Voting System Guidelines. Voluntary voting system standards developed, adopted, and published by the EAC. The guidelines are identified by version number and date.

1.17. Acronyms and Abbreviations. For purposes of this Manual, the acronyms and abbreviations listed below represent the following terms.

Certification Program. The EAC Pilot Voting System Testing and Certification Program

Decision Authority. Testing and Certification Decision Authority

EAC. United States Election Assistance Commission

HAVA. Help America Vote Act of 2002 (42 U.S.C. §15301 et seq.*)*

Labs or Laboratories. Voting System Test Laboratories

NIST. National Institute of Standards and Technology

NVLAP. National Voluntary Laboratory Accreditation Program

Program Director. Director of the EAC Testing and Certification Program

VSTL. Voting System Test Laboratory

VVSG. Voluntary Voting System Guidelines

2. Manufacturer Registration

2.1. Overview. Manufacturer Registration is the process by which voting system Manufacturers make initial contact with the EAC and provide information essential to participate in the EAC Pilot Testing and Certification Program. Before a Manufacturer of a voting system can submit an application to have a pilot voting system certified by the EAC, the Manufacturer must be registered. This process requires the Manufacturer to provide certain contact information and agree to certain requirements of the Certification Program. After successfully registering, the Manufacturer will receive an identification code.

2.2. Registration Required. To submit a voting system for certification or otherwise participate in the EAC Pilot Testing and Certification Program, a Manufacturer must register with the EAC. Registration does not constitute an EAC endorsement of the Manufacturer or its products. Registration of a Manufacturer is not a certification of that Manufacturer's products.

2.3. Registration Requirements. The registration process will require the voting system Manufacturer to provide certain information to the EAC. This information is necessary to enable the EAC to administer the Pilot Certification Program and communicate effectively with the Manufacturer. The registration process also requires the Manufacturer to agree to certain Certification Program requirements. These requirements relate to the Manufacturer's duties and responsibilities under the program. For this program to succeed, it is vital that a Manufacturer know and assent to these duties at the outset of the program.

2.3.1. Information. Manufacturers are required to provide the following information:

2.3.1.1. The Manufacturer's organizational information:

2.3.1.1.1. The official name of the Manufacturer.

2.3.1.1.2. The address of the Manufacturer's official place of business.

2.3.1.1.3. A description of how the Manufacturer is organized (i.e., type of corporation or partnership).

2.3.1.1.4. Names of officers and/or members of the board of directors.

2.3.1.1.5. Names of all partners and members (if organized as a partnership or limited liability corporation).

2.3.1.1.6. Identification of any individual, organization, or entity with a controlling ownership interest in the Manufacturer.

2.3.1.2. The identity of an individual authorized to represent and make binding commitments and management determinations for the Manufacturer (management representative). The following information is required for the management representative:

2.3.1.2.1. Name and title.

2.3.1.2.2. Mailing and physical addresses.

2.3.1.2.3. Telephone number, fax number, and e-mail address.

2.3.1.3. The identity of an individual authorized to provide technical information on behalf of the Manufacturer (technical representative). The following information is required for the technical representative:

2.3.1.3.1. Name and title.

2.3.1.3.2. Mailing and physical addresses.

2.3.1.3.3. Telephone number, fax number, and e-mail address.

2.3.1.4. The Manufacturer's written policies regarding its quality assurance system. This policy must be consistent with guidance provided in the VVSG and this Manual.

2.3.1.5. The Manufacturer's written polices regarding internal procedures for controlling and managing changes to and versions of its voting systems. Such polices shall be consistent with this Manual and guidance provided in the VVSG.

2.3.1.6. The Manufacturer's written polices on document retention. Such policies must be consistent with the requirements of this Manual.

2.3.1.7. A list of all manufacturing and/or assembly facilities used by the Manufacturer and the name and contact information of a person at each facility. The following information is required for a person at each facility:

2.3.1.7.1. Name and title.

2.3.1.7.2. Mailing and physical addresses.

2.3.1.7.3. Telephone number, fax number, and e-mail address.

2.3.2. Agreements. Manufacturers are required to take or abstain from certain actions to protect the integrity of the Pilot Certification Program and promote quality assurance. Manufacturers are required to agree to the following program requirements:

2.3.2.1. Represent a voting system as EAC certified for use in pilot programs only when it is authorized by the EAC and is consistent with the procedures and requirements of this Manual.

2.3.2.2. Notify the EAC of changes to any system previously certified by the EAC pursuant to the requirements of this Manual (see Chapter 3). Such systems shall be submitted for testing and additional certification when required.

2.3.2.3. Permit an EAC representative to verify the Manufacturer's quality control procedures by conducting manufacturing facility audits consistent with Chapter 6 of this Manual.

2.3.2.4. Cooperate with any EAC inquiries and investigations into a certified system's compliance with VVSG standards, other applicable testable requirements or the procedural requirements of this Manual consistent with Chapter 6.

2.3.2.5. Report to the Program Director any known malfunction of a pilot voting system holding an EAC Certification. A malfunction is a failure of a voting system, not caused solely by operator or administrative error, which causes the system to cease operation during a Federal election or otherwise results in data loss. Malfunction notifications should be consolidated into one report. This report should identify the location, nature, date, impact, and resolution (if any) of the malfunction and be filed within 30 days of any Federal election.

2.3.2.6. Certify that the entity is not barred or otherwise prohibited by statute, regulation, or ruling from doing business in the United States.

2.3.2.7. Adhere to all procedural requirements of this Manual.

2.4. Registration Process. Generally, registration is accomplished through use of an EAC registration form. After the EAC has received a registration form and other required registration documents, the agency reviews the information for completeness before approval.

2.4.1. Application Process. To become a registered voting system Manufacturer, one must apply by submitting a Manufacturer Registration Application Form (Appendix A). This form will be used as the means for the Manufacturer to provide the information and agree to the responsibilities required in Section 2.3, above.

2.4.1.1. *Application Form.* In order for the EAC to accept and process the registration form, the applicant must adhere to the following requirements:

2.4.1.1.1. All fields must be completed by the Manufacturer.

2.4.1.1.2. All required attachments prescribed by the form and this Manual must be identified, completed, and forwarded in a timely manner to the EAC (e.g., Manufacturer's quality control and system change policies).

2.4.1.1.3. The application form must be affixed with the handwritten signature (including a digital representation of the handwritten signature) of the authorized representative of the vendor.

2.4.1.2. *Availability and Use of the Form*. The Manufacturer Registration Application Form may be accessed through the EAC web site at www.eac.gov. Instructions for completing and submitting the form are included on the web site. The web site will also provide contact information regarding questions about the form or the application process.

2.4.2. EAC Review Process. The EAC will review all registration applications.

2.4.2.1. After the application form and required attachments have been submitted, the applicant will receive an acknowledgment that the EAC has received the submission and that the application will be processed.

2.4.2.2. If an incomplete form is submitted or an attachment is not provided, the EAC will notify the Manufacturer and request the information. Registration applications will not be processed until they are complete.

2.4.2.3. Upon receipt of the completed registration form and accompanying documentation, the EAC will review the information for sufficiency. If the EAC requires clarification or additional information, the EAC will contact the Manufacturer and request the needed information within 10 business days of receipt of the complete application package.

2.4.2.4. Upon satisfactory completion of a registration application's sufficiency review, the EAC will notify the Manufacturer that it has been registered.

2.5. Registered Manufacturers. After a Manufacturer has received notice that it is registered, it will receive an identification code and will be eligible to participate in the voluntary voting system Certification Program.

2.5.1. Manufacturer Code. Registered Manufacturers will be issued a unique, three-letter identification code. This code will be used to identify the Manufacturer and its products.

2.5.2. Continuing Responsibility To Report. Registered Manufacturers are required to keep all registration information up to date. Manufacturers must submit a revised application form to the EAC within 30 days of any changes to the information required on the application form. Manufacturers will remain registered participants in the program during this update process.

2.5.3. Program Information Updates. Registered Manufacturers will be automatically provided timely information relevant to the Certification Program.

2.5.4. Web site Postings. The EAC will add the Manufacturer to the EAC listing of registered voting system Manufacturers publicly available at www.eac.gov.

2.6. Suspension of Registration. Manufacturers are required to establish policies and operate within the EAC Pilot Program consistent with the procedural requirements presented in this Manual. When Manufacturers engage in management activities that are inconsistent with this Manual or fail to cooperate with the EAC in violation of the Program's requirements, their registration may be suspended until such time as the problem is remedied.

2.6.1. Procedures. When a Manufacturer's activities violate the procedural requirements of this Manual, the Manufacturer will be notified of the violations, given an opportunity to respond, and provided the steps required to bring itself into compliance.

2.6.1.1. *Notice*. Manufacturers shall be provided written notice that they have taken action inconsistent with or acted in violation of the requirements of this Manual. The notice will state the violations and the specific steps required to cure them. The notice will also provide Manufacturers with ten (10) business days (or a greater period of time as stated by the Program Director) to (1) respond to the notice and/or (2) cure the defect.

2.6.1.2. *Manufacturer Action*. The Manufacturer is required to either respond in a timely manner to the notice (demonstrating that it was not in violation of program requirements) or cure the violations identified in a timely manner. In any case, the Manufacturer's action must be approved by the Program Director to prevent suspension.

2.6.1.3. *Non-Compliance*. If the Manufacturer fails to respond in a timely manner, is unable to provide a cure or response that is acceptable to the Program Director, or otherwise refuses to cooperate, the Program Director may suspend the Manufacturer's registration. The Program Director shall issue a notice of his or her intent to suspend the registration and provide the Manufacturer five (5) business days to object to the action and submit information in support of the objection.

2.6.1.4. *Suspension*. After notice and opportunity to be heard (consistent with the above), the Program Director may suspend a Manufacturer's registration. The suspension shall be noticed in writing. The notice must inform the Manufacturer of the steps that can be taken to remedy the violations and lift the suspension.

2.6.2. Effect of Suspension. A suspended Manufacturer may not submit any voting system (pilot or otherwise) for certification under this program. A suspension shall remain in effect until lifted. Suspended Manufacturers will have their registration status reflected on the EAC web site. Manufacturers have the right to remedy a non-compliance issue at any time and lift a suspension consistent with EAC guidance.

3. When Voting Systems Intended for Use in Pilot Programs Must Be Submitted for Testing and Certification

3.1. Overview. An EAC pilot program certification signifies that a voting system has been successfully tested to identified voting system guidelines or testable requirements adopted by the EAC. Only the EAC can issue a Federal certification. Ultimately, systems must be submitted for testing and certification under this program to receive this certification.

3.2. What Is an EAC Certification? Certification is the process by which the EAC, through testing and evaluation conducted by an accredited Voting System Test Laboratory, validates that a voting system meets the requirements set forth specifically for use in pilot programs and performs according to the Manufacturer's specifications for the system. An EAC certification may be issued only by the EAC in accordance with the procedures presented in this Manual.

3.2.1. Types of Voting Systems Certified. The EAC Certification Program is designed to test and certify electromechanical and electronic voting systems submitted for use in pilot programs. Ultimately, the determination of whether a voting system may be submitted for testing and certification under this program is solely at the discretion of the EAC.

3.2.2. Voting System Standards and Testable Requirements. Voting systems certified under this pilot program are tested to a set of voluntary requirements that voting systems must meet to receive a Federal certification. These standards may be the applicable versions of the EAC Voluntary Voting System Guidelines (VVSG) or other testable requirements developed for specific pilot program scenarios.

3.2.2.1. *Versions—Availability and Identification*. Voluntary Voting System Guidelines (or testable requirements) are published by the EAC and are available on the EAC web site (www.eac.gov). The standards will be routinely updated. Versions will be identified by version number and/or release date.

3.2.2.2. *Versions—Basis for Certification***.** The EAC will promulgate which version or versions of the standards or requirements it will accept as the basis for pilot testing and certification programs. **The EAC will certify only those voting systems tested to standards that the EAC has identified as valid for the specific pilot certification effort**.

3.2.3. Significance of an EAC Pilot Certification. An EAC pilot certification is an official recognition that a voting system (in a specific configuration or configurations) has been tested to and has met an identified set of Federal voting system standards or requirements. An EAC certification is **not** any of the following:

3.2.3.1. An endorsement of a Manufacturer, voting system, or any of the system's components.

3.2.3.2. A Federal warranty of the pilot voting system or any of its components.

3.2.3.3. A determination that a pilot voting system, when fielded, will be operated in a manner that meets all HAVA requirements.

3.2.3.4. A substitute for State or local certification and testing.

3.2.3.5. A determination that the system is ready for use in an election.

3.2.3.6. A determination that any particular component of a certified system is itself certified for use outside the certified configuration.

3.2.4. **When Certification Is Required Under the Program**. To obtain an EAC pilot certification, Manufacturers must submit a voting system for testing and certification under this program.

4. Certification Testing, Technical Review and Grant of Certification for Pilot Voting Systems

4.1. Overview. This chapter discusses the procedural requirements for submitting a pilot voting system to the EAC for testing and review. The testing and review process requires an application, employment of an EAC accredited testing laboratory, and technical analysis of the laboratory test report by the EAC. The result of this process is a Decision on Certification by the Decision Authority.

4.2. Policy. Generally, to receive a determination on an EAC certification for a pilot voting system, a registered Manufacturer must have (1) submitted an EAC-approved application for certification, (2) had a VSTL submit an EAC-approved test plan, (3) had a VSTL test a voting system to applicable voting system standards, (4) had a VSTL submit a test report to the EAC for technical review and approval, and (5) received EAC approval of the report in a Decision on Certification.

4.3. Certification Application. The first step in submitting a voting system for certification is submission of an application package. The package contains an application form and a copy of the voting system's Implementation Statement (see VVSG 2005—Version 1.0, Vol. I, Section 1.6.4), functional diagram, and System Overview documentation submitted to the VSTL as a part of the Technical Data Package (see VVSG 2005—Version 1.0, Vol. II, Section 2.2). This application process initiates the certification process and provides the EAC with needed information.

4.3.1. Information on Application Form. The application (application form) provides the EAC certain pieces of information that are essential at the outset of the certification process. This information includes the following:

4.3.1.1. *Manufacturer Information*. Identification of the Manufacturer (name and three-letter identification code).

4.3.1.2. *Selection of Accredited Laboratory*. Selection and identification of the VSTL that will perform voting system testing and other prescribed laboratory action consistent with the requirements of this Manual. Once selected, a Manufacturer may NOT replace the selected VSTL without the express written consent of the Program Director. Such permission will be granted solely at the discretion of the Program Director and only upon demonstration of good cause.

4.3.1.3. *Voting System Standards Information*. Identification of the VVSG, or other EAC approved testable requirements document, including the document's date and version number, to which the Manufacturer wishes to have the identified voting system tested and certified.

4.3.1.4. *Identification of the Pilot Voting System*. Manufacturers must identify the system submitted for testing by providing its name and applicable version number.

4.3.1.5. *Description of the Pilot Voting System*. Manufacturers must provide a brief description of the system being submitted for testing and certification. This description shall include the following information:

4.3.1.5.1. A listing of all components of the system submitted.

4.3.1.5.2. Each component's version number.

4.3.1.5.3. A complete list of each configuration of the system's components that could be fielded as the certified voting system.[1]

4.3.1.5.4. Any other information necessary to identify the specific configuration being submitted for certification.

4.3.1.6. *Date Submitted*. Manufacturers must note the date the application was submitted for EAC approval.

4.3.1.7. *Signature*. The Manufacturer must affix the signature of the authorized management representative.

4.3.2. Submission of the Application Package. Manufacturers must submit a copy of the application form described above and copies of the voting system's (1) Implementation Statement, (2) functional diagram, and (3) System Overview documentation submitted to the VSTL as a part of the Technical Data Package.

4.3.2.1. *Application Form*. Application forms will be available on the EAC web site: www.eac.gov. The application form submitted to the EAC must be signed, dated, and fully, accurately, and completely filled out. The EAC will not accept incomplete or inaccurate applications.

4.3.2.2. *Implementation Statement*. The Manufacturer must submit with the application form a copy of the voting system's Implementation Statement, which must meet the requirements of the VVSG (VVSG 2005—Version 1.0, Vol. I, Section 1.6.4). If an existing system is being submitted with a

[1] An EAC certification applies to the configuration of components (the voting system) presented for testing. A voting system may be fielded without using each of the components that formed the system presented, since voting systems, as certified, may contain optional or redundant components to meet the varying needs of election officials. Systems may not be fielded with additional components or without sufficient components to properly prosecute an election, as neither individual components nor separately tested systems may be combined to create new certified voting systems.

modification, the Manufacturer must submit a copy of a revised Implementation Statement.

4.3.2.3. *Functional Diagram*. The Manufacturer must submit with the application form a high-level Functional Diagram of the voting system that includes all of its components. The diagram must portray how the various components relate and interact.

4.3.2.4. *System Overview*. The Manufacturer must submit with the application form a copy of the voting system's System Overview documentation submitted to the VSTL as a part of the Technical Data Package. This document must meet the requirements of the VVSG (VVSG 2005—Version 1.0, Vol. II, Section 2.2).

4.3.2.5. *Submission*. Applications, with the accompanying documentation, shall be submitted in Adobe PDF, Microsoft Word, or other electronic formats as prescribed by the Program Director. Information on how to submit packages will be posted on the EAC web site: www.eac.gov.

4.3.3. Declaration of Conformity. As part of the application package, Manufacturers must also submit a Declaration of Conformity form described below. This form is included as Appendix B of this Manual and on the EAC web site at www.eac.gov. For the purposes of EAC Pilot Certification Programs, a Declaration of Conformity is the procedure by which a pilot voting system manufacturer notifies and affirms to the EAC that the manufacturer has taken the necessary steps to ensure that the system conforms to the applicable technical standards and requirements promulgated by the EAC for a particular pilot program. All testing done by the manufacturer pursuant to the Declaration of Conformity must either be conducted by the manufacturer themselves under a quality process substantially similar to those noted in ISO/IEC 17025 or by a test laboratory accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) or by the American Association of Laboratory Accreditation (A2LA).

4.3.3.1. *Declaration of Conformity Contents*. The Declaration of Conformity must contain the following information as provided for on the Form:

4.3.3.1.1. Name, address and country designation of the manufacturer.

4.3.3.1.2. Model name/number of the pilot voting system (including a separate attached list of components submitted for the system.

4.3.3.1.3. List of relevant standards/requirements for which the manufacturer is declaring conformity.

4.3.3.1.4. Use Statement. This statement notes that the system must be used according to all the applicable installation, maintenance and use directions provided by the manufacturer.

4.3.3.1.5. Authorized signature, including name, title, and address.

4.3.3.1.6. Date.

4.3.3.2. *Signature Authority*. The Declaration of Conformity must be signed by an individual with the authority to make binding commitments on behalf of the manufacturer. Preferably, the signatory should be an individual in a position to know on behalf of the manufacturer that the voting system complies with the standards/requirements based on the design, manufacture, testing and production control of the pilot voting system.

4.3.3.3. *Declaration of Conformity Record Retention Requirements*. A copy of the Declaration of Conformity and all related documentation will be retained for a period of 5 years after the pilot voting system is no longer manufactured. Such documentation shall be retained on the premises of the manufacturer and must be made available to the EAC consistent with the requirements of Section 6.4 of this Manual. The declaration of conformity shall be kept in a system construction file consisting of at minimum:

4.3.3.3.1. An overall drawing of the system together with drawings of the control circuits.

4.3.3.3.2. Full detailed drawings, accompanied by any calculation notes, test results or other information required to verify that the system conforms to the appropriate standards/requirements.

4.3.4. EAC Review. Upon receipt of a Manufacturer's application package, the EAC will review the submission for completeness and accuracy. If the application package is incomplete, the EAC will return it to the Manufacturer with instructions for resubmission. If the form submitted is acceptable, the Manufacturer will be notified and provided a unique application number within five (5) business days of the EAC's receipt of the application.

4.4. Test Plan. The Manufacturer shall authorize the VSTL identified in its application to submit a test plan directly to the EAC. This plan shall provide for testing of the system sufficient to ensure it is functional and meets all applicable voting system standards. ***For EAC pilot programs, Test Plans must be reviewed and approved before any VSTL testing may commence. (Manufacturer testing used as the basis for the Declaration of Conformity should, of course, be done prior to the submission of an application package by the manufacturer of the pilot voting system seeking EAC certification under this program.)***

4.4.1. Development. An accredited laboratory will develop test plans that use appropriate test protocols, standards, or test suites developed by the laboratory. Laboratories must use all applicable protocols, standards, or test suites issued by the EAC, where applicable.

4.4.2. Required Testing. Test plans shall be developed to ensure that a pilot voting system is functional and meets all requirements of the applicable, approved voting system standards or requirements. The highest level of care and vigilance is required to ensure that comprehensive test plans are created. A test plan should ensure that the voting system meets all applicable standards and that test results and other factual evidence of the testing are clearly documented. System testing must meet the requirements of the VVSG and/or any other requirements developed specifically for pilot program certifications.

.

4.4.3. Format. Test labs shall issue test plans consistent with the requirements in VVSG, Vol. II and any applicable EAC guidance.

4.4.4. EAC Approval. All test plans are subject to EAC approval. No test report will be accepted for technical review unless the test plan on which it is based has been approved by EAC's Program Director.

4.4.4.1. *Review*. All test plans must be reviewed for adequacy by the Program Director. For each submission, the Program Director will determine whether the test plan is acceptable or unacceptable. Unacceptable plans will be returned to the laboratory for further action. Acceptable plans will be approved. All Pilot Program Test Plans will be reviewed by the EAC and either approved or rejected within 7 work days of receipt of the Test Plan.

4.4.4.2. *Unaccepted Plans*. If a plan is not accepted, the Program Director will return the submission to the Manufacturer's identified VSTL for additional action. Notice of unacceptability will be provided in writing to the laboratory and include a description of the problems identified and steps required to remedy the test plan. A copy of this notice will also be sent to the Manufacturer. Questions concerning the notice shall be forwarded to the Program Director in writing. Plans that have not been accepted may be resubmitted for review after remedial action is taken.

4.4.4.3. *Effect of Approval*. Approval of a test plan is required before testing may commence. In most cases, approval of a test plan signifies that the tests proposed, if performed properly, are sufficient to fully test the system. A test plan, however, is approved based on the information submitted. New or additional information may require a change in testing requirements at any point in the certification process.

4.5. Testing. During testing, Manufacturers are responsible for enabling VSTLs to report any changes to a voting system or an approved test plan directly to the EAC. Manufacturers shall also enable VSTLs to report all test failures or anomalies directly to the EAC.

4.5.1. Changes. Any changes to a voting system, initiated as a result of the testing process, will require submission of an updated Implementation Statement, functional diagram, and System Overview document and, potentially, an updated test plan. Test plans must be updated whenever a change to a voting system requires deviation from the test plan originally approved by the EAC. Changes requiring alteration or deviation from the originally approved test plan must be submitted to the EAC (by the VSTL) for approval before the completion of testing. The submission shall include an updated Implementation Statement, functional diagram, and System Overview, as needed. Changes not affecting the test plan shall be reported in the test report. The submission shall include an updated Implementation Statement, functional diagram, and System Overview document, as needed.

4.5.2. Test Anomalies or Failures. Manufacturers shall enable VSTLs to notify the EAC directly and independently of any test anomalies or failures during testing. The VSTLs shall ensure that all anomalies or failures are addressed and resolved before testing is completed. All test failures, anomalies and actions taken to resolve such failures and anomalies shall be documented by the VSTL in an appendix to the test report submitted to the EAC. These matters shall be reported in a matrix, or similar format, that identifies the failure or anomaly, the applicable voting system standards, and a description of how the failure or anomaly was resolved. Associated or similar anomalies/failures may be summarized and reported in a single entry on the report (matrix) as long as the nature and scope of the anomaly/failure is clearly identified.

4.6. Test Report. Manufacturers shall enable their identified VSTL to submit test reports directly to the EAC. The VSTL shall submit test reports only if the voting system has been tested and all tests identified in the test plan have been successfully performed.

4.6.1. Submission. The test reports shall be submitted to the Program Director. The Program Director shall review the submission for completeness. Any reports showing incomplete or unsuccessful testing will be returned to the test laboratory for action and resubmission. Notice of this action will be provided to the Manufacturer. Test reports shall be submitted in Adobe PDF, Microsoft Word, or other electronic formats as prescribed by the Program Director. Information on how to submit reports will be posted on the EAC web site: www.eac.gov.

4.6.2. Format. Manufacturers shall ensure that test labs submit reports consistent with the requirements in the VVSG and this Manual.

4.6.3. Technical Review. A technical review of the test report, technical documents, and test plan will be conducted by EAC technical experts. The EAC may require the submission of additional information from the VSTL or Manufacturer if deemed necessary to complete the review. These experts will submit a report outlining their findings to the Program Director. The report will provide an assessment of the completeness, appropriateness, and adequacy of the VSTL's testing as documented in the test report.

For Pilot Programs, Technical Review will be completed within 10 business days of the receipt of the Test Report by the EAC.

4.6.4. Program Director's Recommendation. The Program Director shall review the report and take one of the following actions:

4.6.4.1. Recommend certification of the candidate system consistent with the reviewed test report and forward it to the Decision Authority for action (Initial Decision); or

4.6.4.2. Refer the matter back to the technical reviewers for additional specified action and resubmission.

4.7. Decision on Certification. Upon receipt of the report and recommendation forwarded by the Program Director, the Decision Authority shall issue a Decision on Certification. The decision shall be forwarded to the Manufacturer consistent with the requirements of this Manual.

4.8. Pre-Certification Requirements. Before a certification is issued for a pilot voting system, Manufacturers must ensure certain steps are taken. They must confirm that the final version of the software that was certified and which the Manufacturer will deliver with the certified system has been subject to a trusted build (see Section 4.9), has been delivered for deposit in an EAC-approved repository (see Section 4.11), and can be verified using Manufacturer-developed identification tools (see Section 4.12). The Manufacturer must provide the EAC documentation demonstrating compliance with these requirements.

4.9. Trusted Build. A software build (also referred to as a compilation) is the process whereby source code is converted to machine-readable binary instructions (executable code) for the computer. A "trusted build" (or trusted compilation) is a build performed with adequate security measures implemented to give confidence that the executable code is a verifiable and faithful representation of the source code. A trusted build creates a chain of evidence from the Technical Data Package and source code submitted to the VSTLs to the actual executable programs that are run on the system. Specifically, the build will do the following:

4.9.1. Demonstrate that the software was built as described in the Technical Data Package.

4.9.2. Show that the tested and approved source code was actually used to build the executable code used on the system.

4.9.3. Demonstrate that no elements other than those included in the Technical Data Package were introduced in the software build.

4.9.4. Document for future reference the configuration of the system certified.

4.10. Trusted Build Procedure. A trusted build is a three-step process: (1) the build environment is constructed; (2) the source code is loaded onto the build environment; and (3) the executable code is compiled and the installation device is created. The process may be simplified for

modification to previously certified systems. In each step, a minimum of two witnesses from different organizations is required to participate. These participants must include a VSTL representative and vendor representative. Before creating the trusted build, the VSTL must complete the source code review of the software delivered from the vendor for compliance with the VVSG and must produce and record file signatures of all source code modules.

4.10.1. Constructing the Build Environment. The VSTL shall construct the build environment in an isolated environment controlled by the VSTL, as follows:

4.10.1.1. The device that will hold the build environment shall be completely erased by the VSTL to ensure a total and complete cleaning of it. The VSTL shall use commercial off-the-shelf software, purchased by the laboratory, for cleaning the device.

4.10.1.2. The VSTL, with vendor consultation and observation, shall construct the build environment.

4.10.1.3. After construction of the build environment, the VSTL shall produce and record a file signature of the build environment.

4.10.2. Loading Source Code onto the Build Environment. After successful source code review, the VSTL shall load source code onto the build environment as follows:

4.10.2.1. The VSTL shall check the file signatures of the source code modules and build environment to ensure that they are unchanged from their original form.

4.10.2.2. The VSTL shall load the source code onto the build environment and produce and record the file signature of the resulting combination.

4.10.2.3. The VSTL shall capture a disk image of the combination build environment and source code modules immediately before performing the build.

4.10.2.4. The VSTL shall deposit the disk image into an authorized archive to ensure that the build can be reproduced, if necessary, at a later date.

4.10.3. Creating the Executable Code. Upon completion of all the tasks outlined above, the VSTL shall produce the executable code.

4.10.3.1. The VSTL shall produce and record a file signature of the executable code.

4.10.3.2. The VSTL shall deposit the executable code into an EAC-approved software repository and create installation disk(s) from the executable code.

4.10.3.3. The VSTL shall produce and record file signatures of the installation disk(s) in order to provide a mechanism to validate the software before installation on the voting system in a purchasing jurisdiction.

4.10.3.4. The VSTL shall install the executable code onto the system submitted for testing and certification before completion of system testing.

4.11. Depositing Software in an Approved Repository. After EAC certification has been granted, the VSTL project manager, or an appropriate delegate of the project manager, shall deliver for deposit the following elements in one or more trusted archive(s) (repositories) designated by the EAC:

4.11.1. Source code used for the trusted build and its file signatures.

4.11.2. Disk image of the pre-build, build environment, and any file signatures to validate that it is unmodified.

4.11.3. Disk image of the post-build, build environment, and any file signatures to validate that it is unmodified.

4.11.4. Executable code produced by the trusted build and its file signatures of all files produced.

4.11.5. Installation device(s) and file signatures.

4.12. System Identification Tools. The Manufacturer shall provide tools through which a fielded voting system may be identified and demonstrated to be unmodified from the system that was certified. The purpose of this requirement is to make such tools available to Federal, State, and local officials to identify and verify that the equipment used in elections is unmodified from its certified version. Manufacturers may develop and provide these tools as they see fit. The tools, however, must provide the means to identify and verify hardware and software. The EAC may review the system identification tools developed by the Manufacturer to ensure compliance. System identification tools include the following examples:

4.12.1. Hardware is commonly identified by model number and revision number on the unit, its printed wiring boards (PWBs), and major subunits. Typically, hardware is verified as unmodified by providing detailed photographs of the PWBs and internal construction of the unit. These images may be used to compare with the unit being verified.

4.12.2. Software operating on a host computer will typically be verified by providing a self-booting compact disk (CD) or similar device that verifies the file signatures of the voting system application files AND the signatures of all nonvolatile files that the application files access during their operation. Note that the creation of such a CD requires having a file map of all nonvolatile files that are used by the voting system. Such a tool must be provided for verification using the file signatures of the original executable files provided for testing. If during the certification process modifications are made and new executable files created, then the tool must be updated to reflect the

file signatures of the final files to be distributed for use. For software operating on devices in which a self-booting CD or similar device cannot be used, a procedure must be provided to allow identification and verification of the software that is being used on the device.

4.13. Documentation. Manufacturers shall provide documentation to the Program Director verifying that the trusted build has been performed, software has been deposited in an approved repository, and system identification tools are available to election officials. The Manufacturer shall submit a letter, signed by both its management representative and a VSTL official, stating (under penalty of law) that it has (1) performed a trusted build consistent with the requirements of Section 4.9 of this Manual, (2) deposited software consistent with Section 4.11 of this Manual, and (3) created and made available system identification tools consistent with Section 4.12 of this Manual. This letter shall also include (as attachments) a copy and description of the system identification tool developed under Section 5.8 above.

4.14. Agency Decision. Upon receipt of documentation demonstrating the successful completion of the requirements above and recommendation of the Program Director, the Decision Authority will issue an Agency Decision granting pilot certification and providing the Manufacturer with a certification number and Certificate of Conformance.

4.15. Certification Document. A Certificate of Conformance will be provided to Manufacturers for voting systems that have successfully met the requirements of the EAC Pilot Program. The document will serve as the Manufacturer's evidence that a particular pilot system is certified to a specific set of testable requirements. The EAC certification and certificate apply only to the specific voting system configuration(s) identified, submitted and evaluated under this Program. Any modification to the system not authorized by the EAC will void the certificate. The certificate will include the product (voting system) name, the specific model or version of the product tested, the name of the VSTL that conducted the testing, identification of the standards to which the system was tested, the EAC certification number for the product, and the signature of the EAC Executive Director. The certificate will also identify the configurations of the voting system's components that may be represented as certified and will specify the date of expiration for the pilot program certification.

4.16. Certification Number. Each pilot system certified by the EAC will receive a certification number that is unique to the system and will remain with the system until the expiration of the pilot program.

4.17. Publication of EAC Certification. The EAC will publish and maintain on its web site a list of all certified pilot voting systems, including copies of all Certificates of Conformance, the supporting test report, and information about the voting system and Manufacturer. Such information will be posted immediately following the Manufacturer's receipt of the EAC Decision and Certificate of Conformance.

4.18. Representation of EAC Certification. Manufacturers may not represent or imply that a pilot voting system is certified unless it has received a Certificate of Conformance for that system.

Statements regarding EAC certification in brochures, on Web sites, on displays, and in advertising/sales literature must be made solely in reference to specific systems. Any action by a Manufacturer to suggest EAC endorsement of its product or organization is strictly prohibited and may result in a Manufacturer's suspension or other action pursuant to Federal civil and criminal law.

4.18.1. **No Mark of Certification Requirement**. Manufacturers are not required to label machines used in EAC Pilot Programs with the EAC Mark of Certification.

5. Denial of Certification

5.1. Overview. When the Decision Authority issues a Decision denying certification of a pilot voting system, the Manufacturer has certain rights and responsibilities. The Manufacturer may request an opportunity to cure the defects identified by the Decision Authority. In addition, the Manufacturer may appeal the decision to the Appeal Authority.

5.2. Applicability of This Chapter. This chapter applies when the Decision Authority makes a Decision to deny an application for pilot voting system certification based on the materials and recommendation provided by the Program Director.

5.3. Form of Decisions. All agency determinations shall be made in writing. Moreover, all materials and recommendations reviewed or used by agency decision makers in arriving at an official determination shall be in written form.

5.4. Effect of Denial of Certification. Upon receipt of the agency's decision denying certification—or in the event of an appeal, subject to the Decision on Appeal—the Manufacturer's application for certification is denied. Such systems will not be reviewed again by the EAC for certification unless the Manufacturer alters the system, retests it, and submits a new application for system certification.

5.5. The Record. The Program Director shall maintain all documents related to a denial of certification. Such documents shall constitute the procedural and substantive record of the decision making process. Records may include the following:

5.5.1. The Program Director's report and recommendation to the Decision Authority.

5.5.2. The Decision Authority's Decision.

5.5.3. Any materials gathered by the Decision Authority that served as a basis for a certification determination.

5.5.4. All correspondence between the EAC and a Manufacturer after the issuance of a Decision denying certification.

5.6. The Decision Authority shall make and issue a written decision on pilot voting systems submitted for certification. Decisions shall be in writing and contain (1) the Decision Authority's basis and explanation for the decision and (2) notice of the Manufacturer's rights in the denial of certification process.

5.6.1. Basis and Explanation. The Decision of the Decision Authority shall accomplish the following:

5.6.1.1. Clearly state the agency's decision on certification.

5.6.1.2. Explain the basis for the decision, including identifying the following:

5.6.1.2.1. The relevant facts.

5.6.1.2.2. The applicable EAC voting system standards or requirements document.

5.6.1.2.3. The relevant analysis in the Program Director's recommendation.

5.6.1.2.4. The reasoning behind the decision.

5.6.1.3. State the actions the Manufacturer must take, if any, to cure all defects in the voting system and obtain a certification.

5.6.2. Manufacturer's Rights. The written Decision must also inform the Manufacturer of its procedural rights under the program, including the following:

5.6.2.1. Right to request a copy or otherwise have access to the information that served as the basis of the Decision ("the record").

5.6.2.2. Right to cure system defects prior to final Agency Decision (see Section 6.8). A Manufacturer may request an opportunity to cure within 10 calendar days of its receipt of the Decision.

5.7. No Manufacturer Action on Decision. If a Manufacturer takes no action (by either failing to request an opportunity to cure) within 10 calendar days of its receipt of the Decision, the Decision shall become the agency's final Decision on Certification. In such cases, the Manufacturer is determined to have foregone its right to cure, and appeal. The certification application shall be considered finally denied.

5.8. Opportunity to Cure. Within 10 calendar days of receiving the EAC's Decision on Certification, a Manufacturer may request an opportunity to cure the defects identified in the EAC's Decision. If the request is approved, a compliance plan must be created, approved, and followed. If this cure process is successfully completed, a pilot voting system denied certification may receive a certification without resubmission.

5.8.1. Manufacturer's Request to Cure. The Manufacturer must send a request to cure within 10 calendar days of receipt of a Decision. The request must be sent to the Program Director.

5.8.2. EAC Action on Request. The Decision Authority will review the request and approve it. The Decision Authority will deny a request to cure only if the proposed plan to cure is inadequate or does not present a viable way to remedy the identified defects within a period of time sufficient to allow the pilot program to move forward. Approval or denial of a request to cure shall be provided the Manufacturer in writing. If the Manufacturer's request to cure is denied, it shall have 10 calendar days from the date it received such notice to request an Appeal of the Agency Decision pursuant to Section 6.9.

5.8.3. Manufacturer's Compliance Plan. Upon approval of the Manufacturer's request for an opportunity to cure, it shall submit a compliance plan to the Decision Authority for approval. This compliance plan must set forth steps to be taken to cure all identified defects. It shall include the proposed changes to the system, updated technical information (as required by Section 4.3.2), and a new test plan created and submitted directly to the EAC by the VSTL The plan shall also provide for the testing of the amended system and submission of a test report by the VSTL to the EAC for approval. It should provide an estimated date for receipt of this test report and include a schedule of periodic VSTL progress reports to the Program Director.

5.8.4. EAC Action on the Compliance Plan. The Decision Authority must review and approve the compliance plan. The Decision Authority may require the Manufacturer to provide additional information and modify the plan as required. If the Manufacturer is unable or unwilling to provide a compliance plan acceptable to the Decision Authority, the Decision Authority shall provide written notice terminating the "opportunity to cure" process.

5.8.5. Compliance Plan Test Report. The VSTL shall submit the test report created pursuant to its EAC-approved compliance plan. The EAC shall review the test report, along with the original test report and other materials originally provided. The report will be technically reviewed by the EAC consistent with the procedures laid out in Chapter 4 of this Manual.

5.8.6. EAC Decision on the System. After receipt of the test plan, the Decision Authority shall issue a decision on a voting system amended pursuant to an approved compliance plan. This decision shall be issued in the same manner and with the same process and rights as a Decision on Certification.

5.9. Appeal of Agency Decision. A Manufacturer may, upon receipt of an Agency Decision denying certification, issue a request for appeal.

5.9.1. Requesting Appeal. A Manufacturer may appeal a decision of the agency by issuing a written request for appeal.

5.9.1.1. *Submission*. Requests must be submitted in writing to the Program Director, addressed to the Chair of the U.S. Election Assistance Commission.

5.9.1.2. *Timing of Appeal*. The Manufacturer may request an appeal within 20 calendar days of receipt of the Agency Decision. Late requests will not be considered.

5.9.1.3. Contents of Request.

5.9.1.3.1. The request must clearly state the specific conclusions of the Decision the Manufacturer wishes to appeal.

5.9.1.3.2. The request may include additional written argument.

5.9.1.3.3. The request may not reference or include any factual material not in the record.

5.9.2. Consideration of Appeal. All timely appeals will be considered by the Appeal Authority.

5.9.2.1. The Appeal Authority shall be two or more EAC Commissioners or other individuals appointed by the Commissioners who have not previously served as the Decision Authority on the matter.

5.9.2.2. All decisions on appeal shall be based on the record.

5.9.2.3. The determination of the Decision Authority shall be given deference by the Appeal Authority. Although it is unlikely that the scientific certification process will produce factual disputes, in such cases, the burden of proof shall belong to the Manufacturer to demonstrate by clear and convincing evidence that its pilot voting system met all substantive and procedural requirements for certification. In other words, the determination of the Decision Authority will be overturned only when the Appeal Authority finds the ultimate facts in controversy highly probable.

5.10. Decision on Appeal. The Appeal Authority shall make a written, Decision on Appeal and shall provide it to the Manufacturer.

5.10.1. Contents. The following actions are necessary to write the Decision on Appeal:

5.10.1.1. State the determination of the agency.

5.10.1.2. Address the matters raised by the Manufacturer on appeal.

5.10.1.3. Provide the reasoning behind the decisions.

5.10.1.4. State that the Decision on Appeal is final.

5.10.2. Determinations. The Appeal Authority may make one of two determinations:

5.10.2.1. *Grant of Appeal.* If the Appeal Authority determines that the conclusions of the Decision Authority shall be overturned *in full*, the appeal shall be granted. In such cases, certification will be approved subject to the requirements of Chapter 4.

5.10.2.2. *Denial of Appeal.* If the Appeal Authority determines that *any part* of the Decision Authority's determination shall be upheld, the appeal shall be denied. In such cases, the application for appeal is finally denied.

5.10.3. Effect. All Decisions on Appeal shall be final and binding on the Manufacturer. No additional appeal shall be granted.

6. Pilot Program Monitoring and Reporting

Overview. The quality of any product, including a voting system, depends on two specific elements: (1) the design of the product or system and (2) the care and consistency of the manufacturing and development process for both hardware and software. Both the Pilot Program and the larger EAC testing and certification process focus on voting system design by ensuring that systems meet the technical specifications of the applicable EAC voting system standards or other applicable testable requirements. This process, commonly called "type acceptance," determines whether the representative sample submitted for testing meets the requirements. What type acceptance does not do is explore whether variations in manufacturing may allow production of non-compliant systems. Generally, the quality of the manufacturing is the responsibility of the Manufacturer. This level of compliance is accomplished by the Manufacturer's configuration management and quality control processes. The EAC's Pilot Program Monitoring and Reporting program, as outlined in this chapter, provides an additional layer of oversight and quality control by allowing the EAC to perform declaration of conformity audits, and to gather information on pilot system anomalies via mandatory reporting from pilot system manufacturers. These tools help ensure that pilot systems meet any and all requirements adopted by the EAC for pilot programs when the systems are manufactured, delivered, and used in Federal election pilot programs.

6.1. Purpose. The purpose of Pilot Program Monitoring and Reporting is to ensure that pilot voting systems certified by the EAC are identical to those fielded in the pilot jurisdictions, to ensure that the voting system manufacturer maintains a rigorous quality management system and to verify that the manufacturer has conducted testing on their product as attested to in the Manufacturer Declaration of Conformity document. This level of monitoring is accomplished primarily by identifying (1) field performance issues with certified systems as reported by the manufacturer and by pilot jurisdictions, (2) manufacturer declaration of conformity audits, and (3) potential EAC observation of pilot programs in operation.

6.2. Manufacturer's Quality Control. EAC's Pilot Program Monitoring functions are not a substitute for the Manufacturer's quality control program. As stated in Chapter 2 of this Manual, all Manufacturers must have an acceptable quality control program in place before they may be registered. The EAC's program serves as an independent check and balance that works in tandem with the Manufacturer's efforts.

6.3. Pilot Program Monitoring Methodology. This chapter provides the EAC with two primary and one secondary tool for assessing the level of compliance to requirements and performance to mission (pilot) objectives of pilot program voting systems. The primary tools are (1) manufacturer declaration of conformity audits and (2) mandatory post election reporting by manufacturers. The secondary tool for monitoring the effectiveness of the program and of the pilot system consists of voluntary pilot program monitoring and reporting by State and local election jurisdiction participating in pilot programs.

6.4. Manufacturer Declaration of Conformity Audit: Manufacturers of pilot voting systems seeking EAC certification will be audited to verify that the system hardware and software being manufactured, shipped, and utilized in the pilot program is the same as the sample

submitted for certification testing. All registered Manufacturers must cooperate with such audits as a condition of program participation.

6.4.1. Notice. The site review will be scheduled during the active testing phase of the pilot certification, at manufacturers' headquarters or manufacturing facility. Scheduling and notice of these audits will be coordinated with and provided to both the manufacturing facility's representative and the Manufacturer's representative.

6.4.2. Pilot Program Audit Objectives. Objectives shall be established for audit programs in order to direct the planning and conduct of all audits conducted under the program. EAC Declaration of Conformity audit objectives will include the following:

6.4.2.1. Gather information and documentation to insure that the attestation in the declaration of conformance agrees with the actual documented testing done on the pilot voting system by the manufacturer.

6.4.2.2. Review documentation (including but not limited to: test plans; test cases, test methods, test suites, test procedures; test data recorded, and test reports) to determine the adequacy of manufacturer conformance testing.

6.4.2.3. Gather information and documentation to insure that the manufacturer adheres to their stated quality management system and configuration management system.

6.4.3. Frequency and Duration. Each manufacturer shall be subject to a mandatory declaration of conformity audit during every pilot certification test engagement. Declaration of conformity audits shall be conducted for a period not to exceed 5 business days.

6.4.4. Records Retention. All documents produced by the manufacturer related to the pilot voting system shall be retained by the manufacturer for a period of ten (10) years in .pdf, .doc, or in some other common format agreed upon by the manufacturer and the EAC. The EAC may at any time, request a copy of such records.

6.4.5. The Audit. Declaration of Conformity audits will generally be conducted in four phases; audit preparation, document review, on site activities and written audit report.

6.4.5.1. Audit Preparation. Prior to the audit, the EAC will develop an audit plan to provide a basis for the conduct of the audit. The plan should also facilitate scheduling and coordination of all audit activities between the manufacturer and the EAC audit team. The audit plan should include:

6.4.5.1.1. The dates and places where the onsite audit activities will be conducted.

6.4.5.1.2. The audit objectives and criteria.

6.4.5.1.3. The expected time and duration of audit activities, including meetings with the manufacturer's representatives.

6.4.5.1.4. Matters related to confidential and proprietary of trade secret information.

6.4.5.2. Document Review. Prior to the audit, documentation shall be collected from the manufacturer for initial review to determine the conformity of the system to the audit criteria. Documentation obtained shall include:

6.4.5.2.1. All technical data package information, system description documentation and users manuals.

6.4.5.2.2. All VSTL testing documentation evidencing system compliance with the appropriate technical requirements and/or standards.

6.4.5.2.3. All internal or external QA audit data from the two most recent audits.

6.4.5.3. On Site Activities. On site audit activities will generally include an opening meeting, collection and verification of information, generating audit findings and exit briefing.

6.4.5.3.1. Opening meeting. An opening meeting will be held between the EAC audit team and senior management and other manufacturer employees as needed. The purpose of the opening meeting is to confirm the audit plan, to provide a summary of how the audit will be conducted, confirm the formal communication channels between the audit team and the manufacturer during the audit and to provide the manufacturer an opportunity to ask questions of the audit team.

6.4.5.3.2. Collect and Verify Information. During the audit, information relevant to the audit scope and objectives should be collected, recorded and verified. Only verifiable evidence may be used to generate audit findings. As time is of the essence in any pilot program test campaign, evidence collected during the audit that suggests an immediate and significant risk of the voting system or manufacturer processes shall be reported to the manufacturer without delay. In instances where the available evidence indicates that the audit objectives are unattainable, the audit team leader shall immediately inform the manufacturer for appropriate action. Such actions may include termination of the audit, or in extreme cases, termination of the pilot testing program pending the manufacturer's appeal as outlined in Chapter 5 of this manual. Sources of information may include the following:

6.4.5.3.2.1. Interviews with manufacturer personnel.

6.4.5.3.2.2. Documents such as policies, procedures, instructions, specifications, drawings, contracts and orders.

6.4.5.3.2.3. Records such as inspection records, audit reports, and results of measurements, data summaries, computerized databases and web sites.

6.4.5.3.2.4. Reports from other sources including customer feedback.

6.4.5.3.2.5. Generate Audit Findings. Evidence collected by the audit team should be evaluated against the audit criteria to generate audit findings. Audit findings can indicate

either conformity or nonconformity with audit criteria. Nonconformities and their supporting evidence should be recorded and reviewed with the manufacturer to verify that the evidence is accurate and that the nonconformities are understood. Every attempt will be made to resolve the accuracy of evidence when the manufacturers' opinion differs from that of the audit team. Any unresolved issues related to the nonconformities should be recorded.

6.4.5.3.3. Exit Briefing. Auditors will present the audit findings and conclusions to the manufacturers' representative or representatives at an exit briefing to be held on the last day of the audit. Audit findings and conclusions will be presented in a manner that is easily understood and acknowledged by the manufacturers' representative. Any differences of opinion regarding the audit findings and conclusions between the audit team and the manufacturers' representative should be discussed and all opinions recorded.

6.4.6. Written Audit Report. A written report documenting the audit findings and conclusions will be drafted by the EAC and provided to the Manufacturer within 10 business days of completion of the audit. The report will detail the findings of the audit, identify actions that are required to correct any nonconformities found during the course of the audit and make a recommendation on whether the manufacturers quality process and the testing performed by the manufacturer appear to meet the requirements outlined in the EAC Standards, Guidelines or Testable Requirements document under which the pilot system is tested. Manufacturers that pass these audits may continue in the pilot certification program. If the audit report finds the manufacturers quality program, and/or product testing was deficient, or if the audit finds that required records were missing, inadequate or otherwise falsified or fabricated in order to circumvent the EAC process, the auditors will recommend that the pilot voting system be dismissed from the pilot program pending adequate resolution of the nonconformities found during the audit.

6.5. Mandatory Post Election Anomaly Reporting. The EAC will require registered manufacturers of voting systems used in pilot programs to collect and submit information related to the performance of the system in any election in which it is used. Information on actual pilot system performance in the field is a basic means for assessing the effectiveness of the pilot product a swell as manufacturing quality control. The EAC will provide a mechanism for election officials to provide real-world input on pilot voting system anomalies.

6.5.1. Post Election Anomaly Report. Manufacturers must record each anomaly that affects the pilot voting system during an election. In addition, the manufacturer shall identify all root causes for each anomaly, and report to the EAC all corrective actions identified

and taken for each anomaly. Reporting of these anomalies will allow the EAC to better evaluate the performance of pilot systems under real election conditions in order to make recommendations for future use of the system. The Report may be filed with the EAC by electronic mail,, by regular mail or by facsimile.

6.5.2. Reported Information. Pilot system manufacturers shall report all voting system anomalies occurring during the election, verify the anomalies to assure that the problem has been properly identified, and evaluate and analyze the anomaly to determine root cause and corrective action. The report must include all of the following information:

6.5.2.1. The manufacturer's name, voting system make and model, and the jurisdiction or jurisdiction in which the anomalies occurred.

6.5.2.2. A narrative description of the anomaly.

6.5.2.3. The affected voting system component, subsystem or software.

6.5.2.4. The action being performed when the anomaly occurred.

6.5.2.5. The number of times the anomalies occurred.

6.5.2.6. Whether the anomaly could be verified.

6.5.2.7. The root cause of the anomaly.

6.5.2.8. The method used to determine the root cause.

6.5.2.9. The corrective and preventative actions taken in response to the anomalies.

6.5.2.10. Any steps taken to validate and verify the effectiveness of the corrective and preventative actions.

6.5.3. Root Cause Analysis. The anomaly report should describe the root cause of the problem or problems identified and the approach taken by the system manufacturer to determine those root causes. Before implementing any corrective actions, the manufacturer should determine the root cause of any anomaly to ensure that the problem is understood. A root cause is the fundamental reason that an anomaly occurred. The root cause, or underlying source of the problem differs from the proximate or direct cause, which is the immediate cause of the problem.
Many problems have multiple root causes leading to the anomaly. In addition, multiple contributing causes can contribute to an anomaly. Causes may include, but are not limited to component or subsystem failures and faults, software errors, human error, design inadequacies and inadequate or non-existent procedures and documentation. Root cause analysis is necessary to properly identify the circumstances and factors leading to an anomaly or anomalies. Without root cause analysis, the likelihood that

only the proximate causes of the anomaly will be fixed increases, so the potential for the anomaly reoccurring remains significant.

6.5.4. Corrective and Preventative Actions. The anomaly report should describe the corrective and preventative actions and the steps taken to validate and verify those actions. A corrective action is a reactive process addressing anomalies that have already occurred. A preventative action is a proactive process taken to stop a potential anomaly from occurring. Verification approaches may include analysis, testing, demonstration and inspection.

6.5.5. Distribution of Post Election Anomaly Reports. All anomaly reports will be posted on the EAC web site in full except where such posting may conflict with the Trade Secrets Act or the release of proprietary and confidential information as discussed in Chapter 9 of this manual.

6.6. Voluntary Anomaly Reporting by States. As another means of gathering field data, the EAC will collect information from election officials who field EAC-certified pilot voting systems. Information on actual voting system field performance is a basic means for assessing the effectiveness of the Certification Program and the manufacturing quality and version control. The EAC will provide a mechanism for State election officials to provide input on their field experiences with the pilot voting system in real-world elections.

6.6.1. Anomaly Report. Election officials may use the Voting System Anomaly Reporting Form to also report pilot voting system anomalies to the EAC. The form and instructions for its completion are available as Appendix C in this Manual or on the EAC Web site, www.eac.gov. The form may be filed with the EAC on line, by mail or by facsimile. Use of the form is required.

6.6.2. Reported Information. Election officials shall report voting system anomalies. An *anomaly* is defined as an irregular or inconsistent action or response from the voting system or system component resulting in some disruption to the election process. Incidents resulting from administrator error or procedural deficiencies are not considered anomalies for purposes of this chapter. The report must include the following information:

6.6.2.1. The official's name, title, contact information, and jurisdiction.
6.6.2.2. A description of the pilot voting system at issue.
6.6.2.3. The date and location of the reported occurrence.
6.6.2.4. The type of election.
6.6.2.5. A description of the anomaly.

6.6.3. Distribution of Reports. State anomaly reports will be posted to the EAC web site and distributed to State and local election jurisdictions, the Manufacturer of the pilot voting system at issue, and the VSTLs.

7. Requests for Interpretations

7.1. Overview. A Request for Interpretation is a means by which a registered Manufacturer or VSTL may seek clarification on a specific EAC pilot voting system standard or requirements document. An Interpretation is a clarification of the pilot voting system standards and guidance on how to properly evaluate conformance to it. This chapter outlines the policy, requirements, and procedures for submitting a Request for Interpretation.

7.2. Policy. Registered Manufacturers or VSTLs may request that the EAC provide a definitive Interpretation of EAC-accepted pilot voting system standards or requirements document when, in the course of developing or testing a voting system, facts arise that make the meaning of a particular standard ambiguous or unclear. The EAC may self-initiate such a request when its agents identify a need for interpretation within the program. An Interpretation issued by the EAC will serve to clarify what a given standard requires and how to properly evaluate compliance. Ultimately, an Interpretation does not amend pilot voting system standards, but serves only to clarify existing standards.

7.3. Requirements for Submitting a Request for Interpretation. An EAC Interpretation is limited in scope. The purpose of the Interpretation process is to provide Manufacturers or VSTLs who are in the process of developing or testing a voting system a means for resolving the meaning of a pilot voting system standard in light of a specific technology without having to present a finished product to EAC for certification. To submit a Request for Interpretation, one must (1) be a proper requester, (2) request interpretation of an applicable voting system standard, (3) present an actual controversy, and (4) seek clarification on a matter of unsettled ambiguity.

7.3.1. Proper Requestor. A Request for Interpretation may be submitted only by a registered Manufacturer or a VSTL. Requests for Interpretation will not be accepted from any other parties.

7.3.2. Applicable Standard. A Request for Interpretation is limited to queries on EAC pilot voting system standards or requirements document. Moreover, a Manufacturer or VSTL may submit a Request for Interpretation only on a version of EAC pilot voting system standards to which the EAC currently offers certification.

7.3.3. Existing Factual Controversy. To submit a Request for Interpretation, a Manufacturer or VSTL must present a question relative to a specific voting system or technology proposed for use in a pilot voting system. A Request for Interpretation on hypothetical issues will not be addressed by the EAC. To submit a Request for Interpretation, the need for clarification must have arisen from the development or testing of a voting system. A factual controversy exists when an attempt to apply a specific section of the Standards or requirements document to a specific system or piece of technology creates ambiguity.

7.3.4. Unsettled, Ambiguous Matter. Requests for Interpretation must involve actual controversies that have not been previously settled. This requirement mandates that interpretations contain actual ambiguities not previously clarified.

7.3.4.1. *Actual Ambiguity*. A proper Request for Interpretation must contain an actual ambiguity. The interpretation process is not a means for challenging a clear EAC pilot voting system standard or requirement. Recommended changes to pilot voting system standards are welcome and may be forwarded to the EAC, but they are not part of this program. An ambiguity arises (in applying a pilot voting system standard to a specific technology) when one of the following occurs:

7.3.4.1.1. The language of the standard is unclear on its face.

7.3.4.1.2. One section of the standard seems to contradict another, relevant section.

7.3.4.1.3. The language of the standard, though clear on its face, lacks sufficient detail or breadth to determine its proper application to a particular technology.

7.3.4.1.4. The language of a particular standard, when applied to a specific technology, clearly conflicts with the established purpose or intent of the standard.

7.3.4.1.5. The language of the standard is clear, but the proper means to assess compliance is unclear.

7.3.4.2. *Not Previously Clarified*. The EAC will not accept a Request for Interpretation when the issue has previously been clarified.

7.4. Procedure for Submitting a Request for Interpretation. A Request for Interpretation shall be made in writing to the Program Director. All requests should be complete and as detailed as possible because Interpretations issued by the EAC are based on, and limited to, the facts presented. Failure to provide complete information may result in an Interpretation that is off point and ultimately immaterial to the issue at hand. The following steps must be taken when writing a Request for Interpretation:

7.4.1. Establish Standing To Make the Request. To make a request, one must meet the requirements identified in Section 7.3 above. Thus, the written request must provide sufficient information for the Program Director to conclude that the requestor is (1) a proper requester, (2) requesting an Interpretation of an applicable pilot voting system standard, (3) presenting an actual factual controversy, and (4) seeking clarification on a matter of unsettled ambiguity.

7.4.2. Identify the EAC Standard or Requirement to be Clarified. The request must identify the specific standard or standards to which the requestor seeks clarification. The request must state the version of the pilot voting system standards at issue (if applicable) and quote and correctly cite the applicable standards.

7.4.3. State the Facts Giving Rise to the Ambiguity. The request must provide the facts associated with the voting system technology that gave rise to the ambiguity in the identified document. The requestor must be careful to provide all necessary information in a clear, concise manner. Any Interpretation issued by the EAC will be based on the facts provided.

7.4.4. Identify the Ambiguity. The request must identify the ambiguity it seeks to resolve. The ambiguity shall be identified by stating a concise question that meets the following requirements:

7.4.4.1. Shall be clearly stated.

7.4.4.2. Shall be related to and reference the pilot voting system standard and voting system technology information provided.

7.4.4.3. Shall be limited to a single issue. Each question or issue arising from an ambiguous standard must be stated separately. Compound questions are unacceptable. If multiple issues exist, they should be presented as individual, numbered questions.

7.4.4.4. Shall be stated in a way that can ultimately be answered *yes* or *no*.

7.4.5. Provide a Proposed Interpretation. A Request for Interpretation should propose an answer to the question posed. The answer should interpret the voting system standard in the context of the facts presented. It should also provide the basis and reasoning behind the proposal.

7.5. EAC Action on a Request for Interpretation. Upon receipt of a Request for Interpretation, the EAC shall take the following action:

7.5.1. Review the Request. The Program Director shall review the request to ensure it is complete, is clear, and meets the requirements of Section 7.4. Upon review, the Program Director may take the following action:

7.5.1.1. *Request Clarification*. If the Request for Interpretation is incomplete or additional information is otherwise required, the Program Director may request that the Manufacturer or VSTL clarify its Request for Interpretation and identify any additional information required.

7.5.1.2. *Reject the Request for Interpretation*. If the Request for Interpretation does not meet the requirements of Section 7.4, the Program Director may reject it. Such

rejection must be provided in writing to the Manufacturer or VSTL and must state the basis for the rejection.

7.5.1.3. *Notify Acceptance of the Request*. If the Request for Interpretation is acceptable, the Program Director will notify the Manufacturer or VSTL in writing and provide it with an estimated date of completion. A Request for Interpretation may be accepted in whole or in part. A notice of acceptance shall state the issues accepted for interpretation.

7.5.2. Consideration of the Request. After a Request for Interpretation has been accepted, the matter shall be investigated and researched. Such action may require the EAC to employ technical experts. It may also require the EAC to request additional information from the Manufacturer or VSTL. The Manufacturer or VSTL shall respond promptly to such requests.

7.5.3. Interpretation. The Decision Authority shall be responsible for making determinations on a Request for Interpretation. After this determination has been made, a written Interpretation shall be sent to the Manufacturer or VSTL. The following actions are necessary to prepare this written Interpretation:

7.5.3.1. State the question or questions investigated.

7.5.3.2. Outline the relevant facts that served as the basis of the Interpretation.

7.5.3.3. Identify the pilot voting system standards interpreted.

7.5.3.4. State the conclusion reached.

7.5.3.5. Inform the Manufacturer or VSTL of the effect of an Interpretation (see Section 9.6).

7.6. Effect of Interpretation. Interpretations are fact specific and case specific. They are not tools of policy, but specific, fact-based guidance useful for resolving a particular problem. Ultimately, an Interpretation is determinative and conclusive only with regard to the case presented. Nevertheless, Interpretations do have some value as precedent. Interpretations published by the EAC shall serve as reliable guidance and authority over identical or similar questions of interpretation. These Interpretations will help users understand and apply the provisions of EAC pilot voting system standards and requirements.

7.7. Library of Interpretations. To better serve Manufacturers, VSTLs, and those interested in the EAC pilot certification program, the Program Director shall publish EAC Interpretations. All proprietary information contained in an Interpretation will be redacted before publication consistent with Chapter 8 of this Manual. The library of published opinions is posted on the EAC web site: www.eac.gov.

8. Release of Certification Program Information

8.1. Overview. Manufacturers participating in a Pilot Certification Program will be required to provide the EAC with a variety of documents. In general, these documents will be releasable to the public. Moreover, in many cases, the information provided will be affirmatively published by the EAC. In limited cases, however, documents may not be released if they include trade secrets, confidential commercial information, or personal information. While the EAC is ultimately responsible for determining which documents Federal law protects from release, Manufacturers must identify the information they believe is protected and ultimately provide substantiation and a legal basis for withholding. This chapter discusses EAC's general policy on the release of information and provides Manufacturers with standards, procedures, and requirements for identifying documents as trade secrets or confidential commercial information.

8.2. EAC Policy on the Release of Pilot Certification Program Information. The EAC seeks to make its Voting System Pilot Program Testing and Certification as transparent as possible. The agency believes that such action benefits the program by increasing public confidence in the process and creating a more informed and involved public. As such, it is the policy of the EAC to make all documents, or severable portions thereof, available to the public consistent with Federal law (e.g. Freedom of Information Act (FOIA) and the Trade Secrets Act).

8.2.1. Requests for information. As in any Federal program, members of the public may request access to Certification Program documents under FOIA (5 U.S.C. §552). The EAC will promptly process such requests per the requirements of that Act.

8.2.2. Publication of documents. Beyond the requirements of FOIA, the EAC intends to affirmatively publish program documents (or portions of documents) it believes will be of interest to the public. This publication will be accomplished through the use of the EAC Web site (www.eac.gov). The published documents will cover the full spectrum of the program, including information pertaining to:

8.2.2.1. Registered Manufacturers;

8.2.2.2. VSTL test plans;

8.2.2.3. VSTL test reports;

8.2.2.4. Agency decisions;

8.2.2.5. Denials of Certification;

8.2.2.6. Issuance of Certifications;

8.2.2.7. Information on a certified voting system's operation, components, features or capabilities;

8.2.2.8. Appeals;

8.2.2.9. Declaration of Conformance Audits and Reporting;

8.2.2.10. Official Interpretations; and

8.2.2.11. Other topics as determined by the EAC.

8.2.3. Trade Secret and Confidential Commercial Information. Federal law places a number of restrictions on a Federal agency's authority to release information to the public. Two such restrictions are particularly relevant to the Certification program: (1) trade secrets information and (2) privileged or confidential commercial information. Both types of information are explicitly prohibited from release by the FOIA and the Trade Secrets Act (18 U.S.C. §1905).

8.3. Trade Secrets. A trade secret is a secret, commercially valuable plan, process, or device that is used for the making or processing of a product and that is the end result of either innovation or substantial effort. It relates to the productive process itself, describing how a product is made. It does not relate to information describing end product capabilities, features, or performance.

8.3.1. The following examples illustrate productive processes that may be trade secrets:

8.3.1.1. Plans, schematics, and other drawings useful in production.

8.3.1.2. Specifications of materials used in production.

8.3.1.3. Voting system source code used to develop or manufacture software where release would reveal actual programming.

8.3.1.4. Technical descriptions of manufacturing processes and other secret information relating directly to the production process.

8.3.2. The following examples are likely not trade secrets:

8.3.2.1. Information pertaining to a finished product's capabilities or features.

8.3.2.2. Information pertaining to a finished product's performance.

8.3.2.3. Information regarding product components that would not reveal any commercially valuable information regarding production.

8.4. Privileged or Confidential Commercial Information. Privileged or confidential commercial information is that information submitted by a Manufacturer that is commercial or financial in nature and privileged or confidential.

8.4.1. Commercial or Financial Information. The terms *commercial* and *financial* should be given their ordinary meanings. They include records in which a submitting Manufacturer has any *commercial interest.*

8.4.2. Privileged or Confidential Information. Commercial or financial information is privileged or confidential if its disclosure would likely cause substantial harm to the competitive position of the submitter. The concept of harm to one's competitive position focuses on harm flowing from a competitor's affirmative use of the proprietary information. It does not include incidental harm associated with upset customers or employees.

8.5. EAC's Responsibilities. The EAC is ultimately responsible for determining whether or not a document (in whole or in part) may be released pursuant to Federal law. In doing so, however, the EAC will require information and input from the Manufacturer submitting the documents. This requirement is essential for the EAC to identify, track, and make determinations on the large volume of documentation it receives. The EAC has the following responsibilities:

8.5.1. Managing Documentation and Information. The EAC will control the documentation it receives by ensuring that documents are secure and released to third parties only after the appropriate review and determination.

8.5.2. Contacting Manufacturer on Proposed Release of Potentially Protected Documents. In the event a member of the public submits a FOIA request for documents provided by a Manufacturer or the EAC otherwise proposes the release of such documents, the EAC will take the following actions:

8.5.2.1. Review the documents to determine if they are potentially protected from release as trade secrets or confidential commercial information. The documents at issue may have been previously identified as protected by the Manufacturer when submitted (see Section 10.7.1 below) or identified by the EAC on review.

8.5.2.2. Grant the submitting Manufacturer an opportunity to provide input. In the event the information has been identified as potentially protected from release as a trade secret or confidential commercial information, the EAC will notify the submitter and allow it an opportunity to submit its position on the issue prior to release of the information. The submitter shall respond consistent with Section 8.6.1 below.

8.5.3. Final Determination on Release. After providing the submitter of the information an opportunity to be heard, the EAC will make a final decision on release. The EAC will inform the submitter of this decision.

8.6. Manufacturer's Responsibilities. Although the EAC is ultimately responsible for determining if a document, or any portion thereof, is protected from release as a trade secret or confidential commercial information, the Manufacturer shall be responsible for identifying documents, or

portions of documents, it believes warrant such protection. Moreover, the Manufacturer will be responsible for providing the legal basis and substantiation for its determination regarding the withholding of a document. This responsibility arises in two situations: (1) upon the initial submission of information; and (2) upon notification by the EAC that it is considering the release of potentially protected information.

8.6.1. Initial Submission of Information. When a Manufacturer is submitting documents to the EAC as required by the Certification Program, it is responsible for identifying any document or portion of a document that it believes is protected from release by Federal law. Manufacturers shall identify protected information by taking the following action:

8.6.1.1. *Submitting a Notice of Protected Information*. This notice shall identify the document, document page, or portion of a page that the Manufacturer believes should be protected from release. This identification must be done with specificity. For each piece of information identified, the Manufacturer must state the legal basis for its protected status.

8.6.1.1.1. Cite the applicable law that exempts the information from release.

8.6.1.1.2. Clearly discuss why that legal authority applies and why the document must be protected from release.

8.6.1.1.3. If necessary, provide additional documentation or information. For example, if the Manufacturer claims a document contains confidential commercial information, it would also have to provide evidence and analysis of the competitive harm that would result upon release.

8.6.1.2. *Label Submissions*. Label all submissions identified in the notice as "Proprietary Commercial Information." Label only those submissions identified as protected. Attempts to indiscriminately label all materials as proprietary will render the markings moot.

8.6.2. Notification of Potential Release. In the event a Manufacturer is notified that the EAC is considering the release of Pilot Program information that may be protected, the Manufacturer shall take the following action:

8.6.2.1. Respond to the notice within 7 calendar days. If additional time is needed, the Manufacturer must promptly notify the Program Director. Requests for additional time will be granted only for good cause and must be made before the 7-day deadline. Manufacturers that do not respond in a timely manner will be viewed as not objecting to release.

8.6.2.2. Clearly state **one** of the following in the response:

8.6.2.2.1. There is no objection to release, or

8.6.2.2.2. The Manufacturer objects to release. In this case, the response must clearly state which portions of the document the Manufacturer believes should be protected from release. The Manufacturer shall follow the procedures discussed in Section 8.6.1 above.

8.7. Personal Information. Certain personal information is protected from release under FOIA and the Privacy Act (5 U.S.C. §552a). This information includes private information about a person that, if released, would cause the individual embarrassment or constitute an unwarranted invasion of personal privacy. Generally, the EAC will not require the submission of private information about individuals. The incidental submission of such information should be avoided. If a Manufacturer believes it is required to submit such information, it should contact the Program Director. If the information will be submitted, it must be properly identified. Examples of such information include the following:

8.7.1. Social Security Number.

8.7.2. Bank account numbers.

8.7.3. Home address.

8.7.4. Home phone number.

Appendix A

Manufacturer Registration Application Form

Available in electronic format at www.eac.gov

U.S. Election Assistance Commission

Print Form | Submit by Email

Manufacturer Registration Application

OMB Control # 3265-0004

1. Manufacturer Information

Legal Name of Business:

Address of Business:

City: **State** Alabama **ZIP Code:**

Organization Type: ☐ Corporation ☐ Partnership ☐ Sole Proprietorship ☐ Other

Names of Officers and/or Board of Directors and/or any and all Partners :

Name of Individual or Entity with Controlling Ownership in the Manufacturer:

2. Management Representative

First Name: **Title:**

Last Name: **Middle Initial:**

Address:

City: **State** Alabama

ZIP Code: **Email:**

Phone Number: **FAX Number:**

3. Technical Representative

First Name: **Title:**

Last Name: **Middle Initial:**

Address:

City: **State** Alabama

ZIP Code: **Email:**

Phone Number: **FAX Number:**

4. **Briefly describe your quality system (e.g. ISO 9001). Provide your written policies supporting this description as a part of this application :**

---

5. **Briefly describe your internal requirements for managing change control/version control for both hardware/firmware and software . Provide your written policies supporting this description as part of this application :**

---

6. **Briefly describe your document retention requirements . Provide your written policies supporting this description as part of this application :**

---

7. **Please, list the Name, Street Address, City, State/Province, Country, Postal Code, and Telephone Number for all facilities used by your company to manufacture your voting system product :**

8. Manufacturer Certification Agreement:

To maintain a voting system certification under the Election Assistance Commission (EAC) program, the manufacturer must agree to:

1. Represent a voting system as certified only when it is authorized by the EAC and consistent with the procedures and requirements of the Testing and Certification Program Manual (the Manual).

2. Produce and permanently affix an EAC certification label to all production units of the certified system.

3. Notify the EAC of changes to any system previously certified by the EAC pursuant to the requirements of the Manual.

4. Permit an EAC representative to verify manufacturer quality control by coordinating with EAC efforts to test and review fielded voting systems consistent with Section 8.6 of the Manual.

5. Permit an EAC representative to verify manufacturer quality control by conducting periodic inspections of manufacturing facilities consistent with Chapter 8 of the Manual.

6. Cooperate with any EAC inquiries and investigations into a certified system's compliance with voting system standards or the procedural requirements of the Manual.

7. Report to the Program Director any known malfunction of a voting system holding a current EAC Certification. A malfunction is defined as a failure of the voting system, not caused by operator or administrative error, which causes the system to fail or otherwise not operate as designed.

8. Certify that the manufacturer is not barred or otherwise prohibited by statute regulation or ruling from doing business in the United States.

9. Adhere to all procedural requirements of the Manual.

Signature:

Title:

Date:

EAC Use Only

Manufacturer's Designation:

Notes:

Instructions:

This form provides for the registration of voting system manufacturers. Registration is the initial required step in the EAC Voting System Certification Program . This form is prescribed by Section 2.4 of the Manual. For more information on registration requirements please see Section 2.4 of the Manual.

This form is generally self-explanatory however the numbers and the instructions below correspond to the numbered sections of the form.

1. Manufacturer Information.

Names of Officers and/or Board of Directors and/or any and all Partners: Ensure that all individuals are identified by name, and title .
Name of Individual or Entity with Controlling Ownership in the Manufacturer: Ensure that the controlling individual is properly named and an address is provided.

2. Management Representative.

Please provide the name and information requested for the designated Manufacturer Representative pursuant to Section 2.3 of the Manual.

3. Technical Representative.
Please provide the name and information requested for the designated Technical Representative pursuant to Section 2.3 of the Manual.

4, 5 and 6
Provide the information listed and attach to your submission the wriiten documentation required by Section 2.3.1 of the Manual.

7. Manufacurer Certification Agreement
Manufacturers are required to take or abstain from certain actions consistent with the certification program. Your concurrence to these requirements is signified by affixing the signature of the manufacturer representative.

This information is required for the EAC to provide for the certification of voting systems as required by 42 U.S.C. Section 15371. This information will be used solely to administer the EAC Testing and Certification Program. This program is voluntary, however, individuals who wish to participate must meet the requirements of the Program. This information will be made public consistent with the requirements of the Freedom of Information Act, the Trade Secrets Act, and any other applicable Federal law or regulation. Public reporting burden for this collection of information is estimated to average about 9.75 hours for completion of this form. This estimate includes the time for reviewing the instructions, gathering information and completing the form. Send comments regarding this burden estimate to the Testing and Certification Program Director, Election Assistance Commission, 1225 New York Avenue, N.W., Suite 1100, Washington, DC 20005. Notwithstanding any other provision of law, no person is required to respond to, nor shall any person be subject to a penalty for failure to respond to, or comply with, a collection of information subject to the requirements of the Paperwork Reduction Act, unless that collection of information displays a currently valid OMB Control Number.

Appendix B

Manufacturer Declaration of Conformity Form

Available in electronic format at www.eac.gov

Print Form

United States Election Assistance Commission

Manufacturer Declaration of Conformity

For EAC Pilot Program Certifications

Manufacturer

Name					
Address					
City		State		Zip Code	
Country					

Product Identification

Model/Type	

See Attached List of components submitted for Conformance Testing for this system

Means of Conformity

The manufacturer hereby declares under his sole responsibility that the products identified with this submission comply with the EAC Pilot Program Testing Standards (listed below by Section or requirement) and with all requirements of the EAC Pilot Program Certification Manual. The technical documentation required to demonstrate that the products meet the requirements noted have been compiled and are available for inspection by the U.S. Election Assistance Commission.

Applicable Standards

Use Statement

Subject to the correct installation, maintenance and use, and to the manufacturers applicable instructions and directions contained in the system Technical Data Package, this system meets all of the EAC requirements for pilot program voting systems.

Authorized Signatory

I, by signing my name below, certify, affirm and acknowledge, under penalty of Federal law, that the claims of conformity attested to in this document are true and accurate.

Signed By

Date

Name

Title

Address

City State Zip Code

Country

Appendix C

Voting System Anomaly Reporting Form

Available in electronic format at www.eac.gov

U.S. Election Assistance Commission

Print Form | Submit by Email

OMB Control # 3265-0004

Voting System Anomaly Reporting Form

For VOLUNTARY reporting of Voting System Anomalies

A. Election Official:

1. **Name, Title, Jurisdiction**

2. **Phone Number**

3. **Email**

4. **Reported to Manufacturer?**

YES ☐ NO ☐

B. Product Description:

5. **Manufacturer Name**

6. **Type of Voting System**

☐ DRE ☐ Ballot Marking Device

☐ Optical Scan ☐ Other

7. **System Model**

8. **Hardware & Software Versions**

9. **Unit Serial Number**

10. **EAC Certification Number**

C. Description of Anomaly or Event:

11. **Date of Occurrence** **Polling Place Name or Location**

12. **Election Type**

☐ Primary ☐ General ☐ Special

13. Was this your first election using this system?

YES ☐ NO ☐

14. **Description of Anomaly**

Instructions

This form provides for the reporting of voting system anomalies by election officials. This form is part of the EAC Quality Monitoring Program. The use of this form is voluntary. Information regarding its use can be found in Section 8.7 of the Manual.

This form is self-explanatory.

This information is required for the EAC to provide for the certification of voting systems as required by 42 U.S.C. Section 15371. This information will be used solely to administer the EAC Testing and Certification Program. This program is voluntary, however, individuals who wish to participate must meet the requirements of the Program. This information will be made public consistent with the requirements of the Freedom of Information Act, the Trade Secrets Act, and any other applicable Federal law or regulation. Public reporting burden for this collection of information is estimated to average about 82 hours for completion of this form. This estimate includes the time for reviewing the instructions, gathering information and completing the form. Send comments regarding this burden estimate to the Testing and Certification Program Director, Election Assistance Commission, 1225 New York Avenue, N.W., Suite 1100, Washington, DC 20005. Notwithstanding any other provision of law, no person is required to respond to, nor shall any person be subject to a penalty for failure to respond to, or comply with, a collection of information subject to the requirements of the Paperwork Reduction Act, unless that collection of information displays a currently valid OMB Control Number.

Attachment E – EAC's Draft UOCAVA Pilot Program Testing Requirements (out for public comment)

UOCAVA PILOT PROGRAM TESTING REQUIREMENTS

Uniformed and Overseas Citizens Absentee Voting Act Pilot Program Testing Requirements

MARCH 24, 2010

Table of Contents

Section 1: Overview 5
1.1 Background 5
1.2 UOCAVA Remote Electronic Voting System Scope 8
1.3 Conformance Clause 10
1.4 Effective Date 14
Section 2: Functional Requirements 15
2.1 Accuracy 15
2.2 Operating capacities 18
2.3 Pre-Voting Capabilities 19
2.4 Voting Capabilities 20
2.5 Post Voting Capabilities 22
2.6 Audit and Accountability 24
2.7 Performance Monitoring 28
Section 3: Usability 29
3.1 General Principles 29
3.2 Alternative Languages 29
3.3 Clarity of Instructions 29
3.4 Voting Input Fields 29
3.5 Interaction Issues 30
3.6 Ballot Legibility 31
3.7 Perceptual Issues 32
Section 4: Software 33
4.1 Selection of Programming Languages 33
4.2 Selection of General Coding Conventions 33
4.3 Software Modularity and Programming 34
4.4 Structured Programming 34
4.5 Comments 35
4.6 Executable Code and Data Integrity 36
4.7 Error Checking 37
4.8 Recovery 39
Section 5: Security 42
5.1 Access Control 42
5.2 Identification and Authentication 45
5.3 Cryptography 48
5.4 Voting System Integrity Management 51
5.5 Communications Security 52
5.6 Logging 54
5.7 Incident Response 60
5.8 Physical and Environmental Security 60
5.9 Penetration Resistance 63
Section 6: Quality Assurance 67
6.1 General Requirements 67
6.2 Components from Third Parties 67
6.3 Responsibility for Tests 67
6.4 Parts and Materials, Special Tests, and Examinations 68
6.5 Quality Conformance Inspections 68
Section 7: Configuration Management 69
7.1 Scope 69
7.2 Configuration Identification 69
7.3 Baseline and Promotion Procedures 70
7.4 Configuration Control Procedures 70
7.5 Configuration Audits 71

Section 8: Technical Data Package 73
8.1 Scope 73
8.2 Implementation Statement 75
8.3 System Hardware Specification 75
8.4 Application Logic Design and Specification 77
8.5 System Security Specifications 89
8.6 System Test Specification 96
8.7 Configuration for Testing 98
Section 9: System Users Manual 100
9.1 Scope 100
9.2 System Overview 100
9.3 System Functionality Description 102
9.4 System Security Specification 103
9.5 Software 105
9.6 Setup Inspection 107
9.7 System Operations Manual 111
9.8 System Maintenance Manual 116
9.9 Personnel Deployment and Training Requirements 119
Appendix A: Definitions of Words with Special Meanings 121
Appendix B: List of References 125
Appendix A: Accuracy Test Case 131

Intentionally left blank

Section 1: Overview

1.1 Background

1.1.1 UOCAVA Pilot Projects

The Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) of 1986 protects the right to vote in federal elections for this defined category of citizens. UOCAVA sets out federal and state responsibilities to assist these voters in exercising their voting rights. The Secretary of Defense is the presidential designee responsible for the federal functions of the Act. The Federal Voting Assistance Program (FVAP) administers this law on behalf of the Secretary of Defense and works cooperatively with other federal agencies and state and local election officials to carry out its provisions.

UOCAVA legislation was enacted before the advent of today's global electronic communications technology. Consequently it relied on U.S. domestic and military mail systems as well as foreign postal systems for the worldwide distribution of election materials. By the mid-1990s it became apparent that the mail transit time and unreliable delivery posed significant barriers for many UOCAVA citizens, preventing them from successfully exercising their right to vote. At the same time the Internet was being widely adopted by businesses, governments and the general public. Therefore it was a natural development for FVAP and states to consider the potential of the Internet as an alternative to the "by-mail" UOCAVA process.

FVAP sponsored Voting Over the Internet (VOI), a small pilot project for the November 2000 general election, to examine the feasibility of using Internet technology. Four states participated in this experiment, which enabled voters to use their own personal computers to securely register to vote, request and receive absentee ballots, and return their voted ballots. Following the successful completion of the VOI project, in the Fiscal Year 2002 National Defense Authorization Act (§1604 of P.L. 107-107:115 Stat.1277), Congress instructed the Secretary of Defense to carry out a larger demonstration project for the November 2002 general election. This project was to be "carried out with participation of sufficient numbers of absent uniformed services voters so that the results are statistically significant".

Since there was not sufficient time to define and implement a large project for 2002, the project was planned for implementation for the November 2004 election. Seven states agreed to participate and worked with FVAP to develop system requirements and operating procedures. However, the Secure Electronic Registration and Voting Experiment (SERVE) was cancelled before it was deployed due to concerns raised by several computer scientists. These individuals contended that the use of personal computers over the Internet could not be made secure enough for voting and consequently called for the project to be terminated. The Department of Defense, citing a lack of public confidence in the SERVE system, decided the project could not continue under these circumstances.

In response to this development, the Fiscal Year 2005 National Defense Authorization Act (§567 of P.L. 108-375;118 Stat.119) repealed the requirement for the Secretary of Defense to conduct an electronic voting

demonstration project “until the first regularly scheduled general election for federal office which occurs after the Election Assistance Commission (EAC) notifies the Secretary that the Commission has established electronic absentee voting guidelines and certifies that it will assist the Secretary in carrying out the project”. Pursuant to this legislation, in September 2005, the EAC requested its voting system advisory group, the Technical Guidelines Development Committee (TGDC), to add this subject on their research agenda; however the request was declined.

Since the State of Florida conducts its own voting system certification process, Okaloosa County, Florida, decided to field a small pilot for the 2008 general election. Instead of allowing voters to use their own personal computers, Okaloosa County set up staffed absentee voting locations in England, Germany and Japan. Voters that visited these sites were allowed to cast their ballots electronically using laptop computers supplied by the Supervisor of Elections office. Election workers that staffed these sites verified voter identity and eligibility using an on-line connection to the voter registration system. A paper record of each vote was printed and used to verify the electronic results when the votes were tabulated.

1.1.2 Testing Pilot Systems

Most states require voting systems to undergo a testing and certification process before the system may be used in an election. This provides a level of assurance that the system provides the required functionality and operates reliably and securely. The four states participating in the VOI project agreed to test that system utilizing the Department of Defense Information Technology Security Certification and Accreditation (DITSCAP) process combined with the State of Florida Division of Elections Voting Systems Certification process. The testing regimen planned for the SERVE system was a combined DITSCAP, National Association of State Election Directors (NASED), and State of Florida certification and accreditation process. The system used for Okaloosa County’s remote voting pilot was tested and certified by the State of Florida Division of Elections.

Due to the nature of these new systems, existing voting system standards were not sufficient for testing specific aspects. Therefore, additional security requirements were needed to test the use of digital signatures, cryptography and secure communications protocols. The hardware and software standards, developed for DRE and optical scan systems used in polling places, also needed to be revised to reflect the characteristics of the remote voting technologies. Each of the pilot projects established a working group, comprised of election officials, security experts and test engineers, to define the additional requirements needed to supplement the existing voting system standards. Reference materials for the working groups came from various national and international sources of information technology standards, such as the Federal Information Processing Standards (FIPS), Common Criteria, and the International Standards Organization. These efforts resulted in testing requirements documents that were specific to the technical features of each of the pilot systems, which supplied the criteria for testing and certifying these particular pilot systems.

Since 2008, several states have enacted legislation enabling them to conduct electronic voting projects for UOCAVA voters, beginning with the 2010 elections. To be prepared to support the states with these projects, in July

2009 the EAC convened a UOCAVA Working Group to consider how to adapt the EAC's Testing and Certification Program to accommodate UOCAVA pilot systems. It was concluded that two products were needed: a modified set of system testing requirements; and a revised testing and certification process. It was determined that the working group would assist the EAC in drafting the testing requirements and EAC staff would adapt the certification process to accommodate the UOCAVA pilot program.

The EAC UOCAVA Working Group has taken much the same approach as the pilot project working groups. The source materials drawn on for this effort included: the Voluntary Voting System Guidelines (VVSG) 1.0 ; the VVSG 1.1; the VVSG 2.0; the VOI, SERVE and Okaloosa Project requirements documents; FIPS; and NIST Special Publications. One significant difference in the EAC Working Group approach was the technology scope covered by the requirements. The VOI, SERVE and Okaloosa system requirements were tailored specifically for the particular system implementations developed for those projects. However, since many different types of remote voting systems could be submitted to the EAC certification program, the EAC Working Group defined generic system requirements to provide for system design flexibility.

1.1.3 Scope of EAC Pilot Project Testing Requirements

Pilot projects are small in scale and short in duration. Consequently, certification for pilot systems needs to be quicker and less expensive than the regular process currently used for conventional systems with an expected life of more than 10 years. Nevertheless, since actual votes will be cast using the voting systems utilized in the pilot project, the certification process must retain sufficient rigor to provide reasonable assurance that the pilot systems will operate correctly and securely.

There is a fundamental dichotomy in complexity in remote voting architectures: those where the voting platform is controlled (e.g., provided by the election jurisdiction); and those where it is not controlled (e.g., the voter uses his own personal computer). Since the EAC planned to have the pilot certification process ready for implementation during the first half of 2010, it was decided that the EAC would focus its efforts on controlled platform architectures servicing multiple jurisdictions. This is a highly secure remote voting solution and the Okaloosa Project provides an implementation example for reference. Defining requirements for this class of system architecture was determined to provide a reasonable test case that could be completed within the available timeframe. In addition, most of the core system processing functions are the same for both types of architectures, so a substantial number of requirements will carry over as this work is expanded to include other methods of remote electronic voting.

1.1.4 Next Steps

While the EAC was working to ensure that the pilot certification effort was underway, legislation dealing with a number of UOCAVA voting issues were under consideration by Congress. Ultimately, passed as part of the Fiscal Year 2010 National Defense Authorization Act (NDAA) (§581 of P.L. 111-84), the Military and Overseas Voters Empowerment Act contains a provision allowing the Secretary of Defense to establish one or more pilot programs to test the feasibility of new election technology for UOCAVA voters. This provision requires the EAC and the National Institute of Standards and Technology (NIST) to provide best practices or standards to support these pilot programs,

"in accordance with electronic absentee voting guidelines established under" the earlier FY2005 NDAA. In December 2009, the EAC directed the TGDC to begin this work as a top research priority. The EAC expects this work to result in the comprehensive set of remote electronic voting system guidelines as mandated by the FY2005 NDAA. The TGDC has been tasked to consider the full range of remote voting architectures, including instances where the voter can use his own personal computer for voting. The pilot testing requirements, that the EAC is currently developing, will be provided to the TGDC as the basis and starting point for their research and deliberations.

1.2 UOCAVA Remote Electronic Voting System Scope

An initial step in a system certification process is to define the scope of what should be included in the certification. UOCAVA pilot project systems operate as adjuncts to the various polling site systems used by the jurisdictions that are participating in the pilot project. The systems will require linkages to the local Election Management System in order to obtain election definition data and to report election results. The systems also will require linkages to the Voter Registration Database to authenticate voters and determine their eligibility to vote, match them with the correct ballot style, and record voter history. Processes that are handled procedurally for polling place systems may be implemented in a software application in a remote electronic system. Another difference is that the UOCAVA voting period currently extends for 45 days. So these absentee systems have to be in operation for a fairly long time before polling places are open. Most, if not all, states prohibit tabulation of absentee ballots until the polls are closed, so voted ballots may have to be stored on the system for several weeks. Therefore, the functions and the architectures of remote voting systems demonstrate some notable differences from conventional polling site systems.

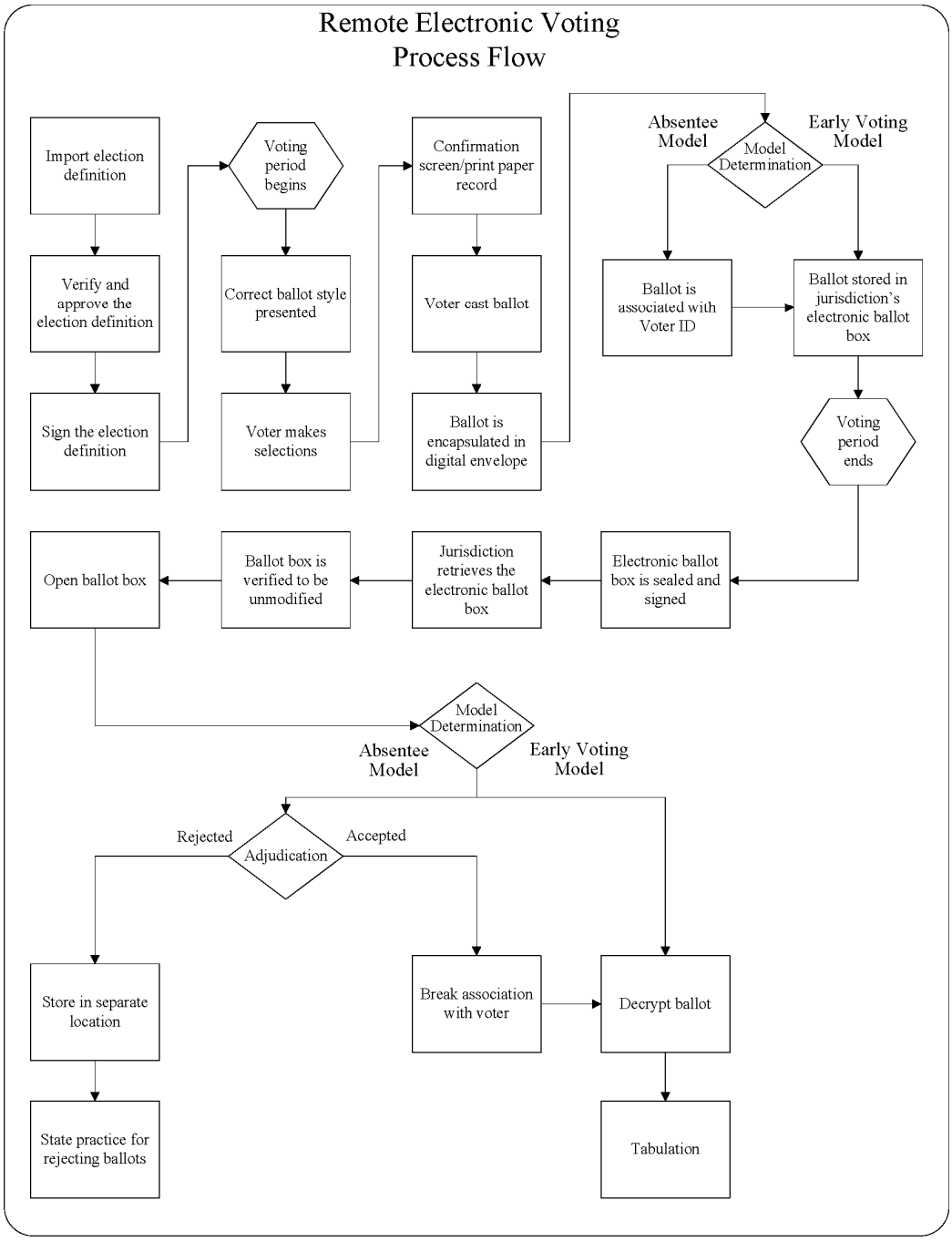
Figure 1-1 illustrates a generic process flow for remote electronic voting that does not presuppose any particular architectural solution. Even at this high level of abstraction, two alternative processing paths are needed to accommodate differences in individual state requirements. The first path, called the absentee model, has two distinguishing features. This is essentially an electronic rendering of the UOCAVA by-mail process. In this path, the voter's identity must remain linked to the cast ballot until the close of the voting period. At that time an adjudication is made by the local jurisdiction on whether to accept or not accept the ballot. If the ballot is accepted, any identifiable link to the voter is removed. The now anonymous ballot is placed in the ballot box to be tabulated. If the ballot is rejected, the link is not removed and the disposition of the 'unopened' ballot is made in accordance with individual state procedures.

The second path, called the early voting model, does not maintain any association between the voter and the cast ballot. When the voter presses the 'Vote' button and receives notification that the ballot has been recorded, the ballot goes directly into the ballot box. There is no ballot adjudication step and therefore no need to maintain a connection between the voter and the ballot.

There are many of ways in which systems can be designed to perform these absentee functions. However, as noted in 1.1, only one type of system architecture is covered in this document. The voting platform envisioned is a remote voting location staffed and managed by election workers, which services a number of different election jurisdictions. The election workers verify the voter's identity and eligibility to vote and update voter history in much the same manner as poll workers perform these functions at a polling place. The voter uses a laptop computer or similar device

provided by the project to view the ballot, make his selections and cast his ballot. For security purposes, no vote data is permanently retained by the voting device. The cast ballot is transmitted to an electronic ballot box which is stored at another location. The voting device is equipped with a printer to produce a paper record of the voter's choices that the voter can review for verification purposes. The paper record must be deposited in a secure receptacle and transported to the appropriate jurisdiction for system audit purposes. Other elements of the system architecture are not specified. All systems submitted for pilot certification must support both the absentee and the early voting models.

Figure 1-1 UOCAVA Process



1.3 Conformance Clause

1.3.1 Scope and Applicability

This document defines requirements for conformance of remote electronic voting systems intended for use in UOCAVA pilot programs that manufacturers of such systems SHALL meet pursuant to EAC pilot program certification. These pilot programs consist of staffed kiosks connected to multiple state data centers with paper records to support system performance validation. Pilot system functionality excludes voter registration and election management system except for defined data interchange interfaces. This document also provides the framework, procedures, and requirements that voting system testing labs (VSTLs) and manufacturers responsible for the certification testing of such pilot program systems SHALL follow. The requirements and procedures in this document may also be used by states to certify remote electronic voting systems for their own pilot programs.

This document defines the minimum requirements for remote electronic voting systems in the context of pilot programs conducted by states and local jurisdictions and the process of testing these systems. The requirements are intended for use by:

- Designers and manufacturers of voting systems;
- VSTLs performing the analysis and testing of systems in support of the EAC certification process;
- Election officials, including ballot designers and officials responsible for the installation, operation, and maintenance of voting machines for UOCAVA pilot programs; and
- VSTLs and consultants performing the state certification of voting systems for pilot programs.

Minimum requirements specified in this document include:

- Functional capabilities;
- Performance characteristics, including security;
- Documentation; and
- Test evaluation criteria.

1.3.2 Conformance Framework

This section provides the framework in which conformance is defined. It identifies the entities to which these requirements apply, the relationships among the various entities, the structure of the requirements, and the terminology used to indicate conformance.

1.3.2.1 Applicable entities

The requirements, prohibitions and options specified in these requirements apply to remote electronic voting systems, voting system manufacturers, and VSTLs. These requirements apply to all systems submitted for pilot certification under the EAC program.

1.3.2.2 Requirements of entities

It is the voting system manufacturer that must implement these requirements and provide the necessary documentation for the system. In order to claim conformance to the requirement, the voting system manufacturer SHALL satisfy the specified requirements. The voting system manufacturer SHALL successfully complete the prescribed test campaign with an EAC VSTL in order to obtain EAC certification.

The VSTL SHALL satisfy the requirements for conducting pilot program certification testing. Additionally, as indicated in the document, certain requirements SHALL be tested by the manufacturer rather than the VSTL. The VSTL may use an operational environment emulating that used by election officials as part of their testing to ensure that the voting system can be configured and operated in a secure and reliable manner according to the manufacturer's documentation and as specified by the requirements. The VSTL SHALL coordinate and deliver the requisite documentation, including a Test Plan and a Test Report, to the EAC for review and approval.

The EAC SHALL review the test results and associated documentation from both the VSTL and the manufacturer and make a determination that all requirements have been appropriately tested and the test results are acceptable. The EAC may conduct audits of manufacturer testing to ensure its adequacy. The EAC will issue a pilot program certification number that indicates conformance of the specified system to these requirements.

1.3.3 Extensions

Extensions are additional functions, features, and/or capabilities included in a voting system that are not required by this document. To accommodate the needs of states that may impose additional requirements and to accommodate changes in technology, this document allows extensions. The use of extensions SHALL NOT contradict nor cause the nonconformance of functionality required by this document.

1.3.4 Implementation Statement

The implementation statement SHALL describe the remote electronic voting system and SHALL document the requirements that have been implemented by the voting system. It SHALL also identify optional features and capabilities supported by the voting system, as well as any extensions (i.e., additional functionality beyond what is required in this document). The implementation statement SHALL include a checklist identifying all the requirements for which a claim of conformance is made.

The implementation statement SHALL be submitted with the manufacturer's application to the EAC for pilot program certification testing. It SHALL provide a concise summary and narrative description of the voting system's capabilities. It SHALL include identifying information about the voting system, including the hardware and software components, version number and date.

1.3.5 Equivalent Configurations

1.3.5.1 Background

Under the current EAC certification program (prior to this document), the scope of certification is very specific and extends only to the exact voting system configuration tested. The certificate specifically identifies each of the various configurations of the voting system's components that were tested and certified, including the OS version and service pack, as well as the CPU. Any modification to the system not authorized by the EAC will void the certificate. The certificate is applicable to the system configuration that has been tested during certification and is not applicable when any modification to hardware, software or COTS products has occurred.

There is a tradeoff between requiring the exact configuration that was tested and certified to be deployed and allowing "equivalent configurations" that have been tested by the voting system manufacturer and attested to perform identically on these configurations. Requiring only exact configurations that have been certified to be deployed guarantees that the customer is using the actual system that has been tested by the VSTL, but does not allow the flexibility needed to accommodate routine and expected changes to COTS systems. The requirements in this document are designed to allow for such flexibility.

1.3.5.2 Procedures for changes to baseline configuration

Testing for UOCAVA Pilot Certification is conducted by the VSTL and voting system manufacturer on the baseline configuration consisting of:

1. Specific hardware;
2. Major Version of operating system and third-party COTS applications.
    - Major Versions are changed when an updated version is downloaded; major versions are not considered changed when a patch is applied to fix an individual item.
    - In Microsoft Operating Systems, Major Versions would include Service Packs– New Service Packs would be considered a different Major Version.
    - Downloading patches (i.e., security) would not be considered a change to the Major Version. However, manufacturers SHALL create a log of all patches downloaded and supply them to the EAC upon request.

Any change to hardware or software (Major Versions) SHALL be regression tested by the voting system manufacturer to ensure that all requirements affected by the change have been adhered to. Regression testing SHALL be documented and legally affirmed to by the manufacturer, and accepted by the EAC. Regression testing SHALL be done by the manufacturer when the EAC certified version differs from the one being deployed in any of the following ways:

a. Any hardware is changed. However, de minimis changes, as defined in the EAC Certification Manual, SHALL NOT undergo regression testing;

b. Any change to Major Version of the OS is made; and

c. Any major change to a third-party COTS application is made.

All regression testing by manufacturers SHALL include accuracy and reliability testing. Other tests SHALL be repeated for requirements closely related to the functionality that was modified with the hardware or software (Major Version) changes.

Any change to the voting system application not covered by 3 a, b or c SHALL undergo testing by the VSTL.

Test Reports describing the manufacturer regression testing SHALL be submitted to the EAC. The EAC may conduct random audits to ensure that the manufacturer regression testing performed was sufficient.

1.3.6 Requirements Language and Structure

1.3.6.1 Language

Understanding how language is used is a pre-requisite to understanding this document. Language in this document is divided into two categories: normative, i.e., the requirements language itself, and informative. Normative language is prescriptive and must be followed to obtain conformance to this document and ultimately EAC certification. Informative parts of this document include discussion, examples, extended explanations, and other matter that are necessary for proper understanding of the requirements and how to ensure conformance. Informative text is not prescriptive and serves to clarify requirements.

Normative language is specifically for requirements. The following keywords are used within requirements text to indicate the conformance aspects of the requirement:

- SHALL indicates a mandatory requirement to do something;
- SHALL NOT indicates a mandatory requirement not to do something.

1.3.6.2 Structure of requirements

Each remote electronic voting system requirement in this document is identified according to a hierarchical scheme in which higher-level requirements (e.g., "Voter SHALL make application to request to vote absentee by remote electronic method") are supported by lower-level requirements (e.g., "The application SHALL include name, date of birth, legal residence address, etc."). Thus, requirements are nested. When the nesting hierarchy has reached four levels (i.e., 1.1.1.1), further nested requirements are designated with lowercase letters, then roman numerals. Therefore, all requirements are traceable by a distinct reference.

Some requirements are directly testable and some are not. Lower-level requirements (i.e., leaf-node requirements that have no requirements directly beneath them) are directly testable. Higher-level requirements (i.e., requirements with directly testable requirements beneath them) are not directly testable. Higher-level requirements are included because: (1) they are testable indirectly insofar as their lower-level requirements are testable; and (2) they often provide the structure and rationale for the lower level requirement. Satisfying all the lower-level requirements will

result in satisfying the corresponding higher-level requirement. Thus, VSTLs need to only directly test lower-level requirements, not higher-level requirements. However, if non-conformance with a higher-level requirement is determined through any other means (e.g., OEVT testing, inspection, etc.) then the voting system is deemed not to conform to that higher-level requirement.

1.4 Effective Date

The UOCAVA Pilot Program Testing requirements SHALL become effective for pilot certification testing upon adoption by the EAC. At that time, all pilot systems submitted for EAC certification SHALL be tested for conformance with these requirements.

These requirements are voluntary in that each of the states can decide whether to require the voting systems used in pilot programs for their state to have an EAC certification. States may decide to adopt these requirements in whole or in part at any time, irrespective of the effective date. In addition, states may specify additional requirements that pilot voting systems used in their jurisdictions must meet. The EAC certification program does not, in any way, pre-empt the ability of the states to have their own voting system certification process.

Section 2: Functional Requirements

2.1 Accuracy

Voting system accuracy addresses the accuracy of data for each of the individual ballot selections that could be selected by a voter, including the positions that are not selected. Accuracy is defined as the ability of the voting system to capture, record, store, consolidate and report the specific selections and absence of selections, made by the voter on each ballot without error.

For each processing function in the following list, the voting system 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. Types of functions include:

- Recording voter selections of candidates and contest into voting data storage;
- Recording voter selections into ballot image storage independently from voting data storage; and
- Consolidation of vote selection data from multiple voting sites to generate jurisdiction-wide vote totals.

2.1.1 Components and Hardware

2.1.1.1 Component accuracy

Memory hardware, such as semiconductor devices and magnetic storage media, SHALL be accurate.

Test Method: ***Functional***

Test Entity: ***VSTL***

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.

Test Method: ***Functional***

Test Entity: ***VSTL***

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.

Test Method: ***Functional***

Test Entity: ***VSTL***

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.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.1.3 Content of Data Verified for Accuracy

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.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.1.3.2 Recording accuracy

For recording accuracy, all voting systems SHALL:

a. Record every entry made by the user;

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.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.1.4 Telecommunications Accuracy

The telecommunications components of all voting systems SHALL meet the requirements specified in section 2.1.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.1.5 Accuracy Test Content

Voting system accuracy SHALL be verified by a specific test conducted for this objective. The overall test approach is described in Appendix C.

2.1.5.1 Simulators

If a simulator is used, it SHALL be verified independent of the voting system in order to produce ballots as specified for the accuracy testing.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.1.5.2 Ballots

Ballots used for accuracy testing SHALL include all the supported types (i.e., rotation, languages, etc.) of contest and election types (primary, general)

Test Method: ***Functional***

Test Entity: ***VSTL***

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.

UOCAVA voting systems SHALL produce reports that are consistent with no discrepancy among reports of voting data.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.2 Operating capacities

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, communications links):

- Throughput,
- Memory,
- Transaction processing speed, and
- Election constraints:
  - Number of jurisdictions
  - Number of ballot styles per jurisdictions
  - Number of contests per ballot style
  - Number of candidates per contest

Test Method: ***Functional***

Test Entity: ***VSTL***

2.2.1.1 Capacity testing

The voting system SHALL achieve the maximum operating capacities stated by the manufacturer in section 2.2.1

Test Method: ***Functional***

Test Entity: ***VSTL***

2.2.2 Operating Capacity notification

The voting system SHALL provide notice when any operating capacity is approaching its limit.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.2.3 Simultaneous Transmissions

The voting system SHALL protect against the loss of votes due to simultaneous transmissions.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.3 Pre-Voting Capabilities

2.3.1 Import and Verify Election Definition

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 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.

Test Method: ***Inspection/Functional***

Test Entity: ***VSTL***

2.3.1.2 Protect the election definition

The voting system SHALL provide a method to protect the election definition from unauthorized modification.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.3.2 Readiness Testing

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.

Test Method: ***Functional***

Test Entity: ***VSTL***

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.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.4 Voting Capabilities

2.4.1 Opening the Voting Period

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.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.4.2 Casting a Ballot

2.4.2.1 Record voter selections

The voting system SHALL:

a. Record the selection and non-selection of individual vote choices for each contest and ballot measure;

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 select his preferences on the ballot in any legal number and combination;

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. Prevent the voter from making more than the allowable number of selections for any contest (e.g., overvotes); and

i. 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.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.4.2.2 Verify voter selections

The voting system SHALL:

a. Generate a paper record identifier. This SHALL be a random identifier that uniquely links the paper record with the cast vote record;

b. Produce a paper record each time the confirmation screen is displayed;

c. After reviewing the confirmation screen and paper record, a voter SHALL be able to either cast the ballot or return to the vote selection process to make changes; 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.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.4.2.3 Cast ballot

The voting system SHALL:

a. Store all cast ballots in a random order;

b. Notify the voter after the vote has been stored successfully that the ballot has been cast;

c. Notify the voter that the ballot has not been cast successfully if it is not stored successfully, including storage of the ballot, 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.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.4.2.4 Ballot linking to voter identification

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.

Test Method: Functional

Test Entity: VSTL

2.4.2.4.2 Early voting model

The cast ballot SHALL NOT be linked to the voter's identity.

Test Method: Inspection

Test Entity: VSTL

2.4.3 Vote Secrecy

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.

Test Method: Functional

Test Entity: VSTL

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.

Test Method: Functional

Test Entity: VSTL

2.5 Post Voting Capabilities

2.5.1 Ballot Box Retrieval and Tabulation

2.5.1.1 Seal and sign the electronic ballot box

The voting system SHALL seal and sign the electronic ballot box, by means of a digital signature, to protect the integrity of its contents.

Test Method: Functional

Test Entity: VSTL

2.5.1.2 Electronic ballot box retrieval

The voting system SHALL allow each jurisdiction to retrieve its electronic ballot box.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.5.1.3 Electronic ballot box integrity check

The voting system SHALL perform an integrity check on the electronic ballot box verifying that is has not been tampered with or modified before opening.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.5.1.4 Open ballot box

The voting system SHALL allow only an authorized entity to open the ballot box.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.5.1.5 Absentee model

2.5.1.5.1 Adjudication

The voting system SHALL allow the designation of electronic ballots as “accepted” or “not accepted” by an authorized entity.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.5.1.5.2 Digital envelope removal

After a ballot is accepted, the voting system SHALL remove the digital envelope breaking all correlation between the voter and the ballot.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.5.1.6 Ballot decryption

The decryption process SHALL remove all layers of encryption, producing a record that is in clear text.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.5.2 Tabulation

2.5.2.1 Tabulation report format

The voting system SHALL have the capability to generate a tabulation report of voting results in an open and non-proprietary format.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.6 Audit and Accountability

2.6.1 Scope

This section presents requirements for the voting system to provide the capability for certain types of audits listed below. The audits work together to ensure independent agreement between what is presented to the voters by the paper record and the electronic tabulation results. The audits addressed in this section are:

a. Hand audit - Validate electronic tabulation results ballot style through comparison with results of manual count of paper records; and

b. Random sampling comparison of ballot images and the corresponding paper records.

2.6.2 Electronic Records

In order to support independent auditing, a voting system SHALL be able to produce electronic records that contain the necessary information in a secure and usable manner. Typically, this includes records such as:

- Vote counts;
- Counts of ballots recorded;
- Paper record identifier;
- Event logs and other records of important events; and
- Election archive information.

The following requirements apply to records produced by the voting system for any exchange of information between devices, support of auditing procedures, or reporting of final results:

a. Requirements for which electronic records must be produced by tabulators; and

b. Requirements for printed reports to support auditing steps.

2.6.2.1 All records capable of being exported

The voting system SHALL provide the capability to export its electronic records.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.6.2.2 Ballot images

The voting system SHALL have the capability to generate ballot images in a human readable format.

Test Method: ***Functional***

Test Entity: ***VSTL***

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-ins.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.6.2.4 All records capable of being printed

The voting system 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.

Test Method: ***Functional***

Test Entity: ***VSTL***

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.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.6.3 Paper Records

The vote capture device is required to produce a paper record. This record SHALL be available to the voter to review and verify, and SHALL be retained for later auditing or recounts, as specified by state law. Paper records provide an independent record of the voter's choices that can be used to verify the correctness of the electronic record created by the voting device.

2.6.3.1 Paper record creation

Each vote capture device SHALL print a human readable paper record.

Test Method: ***Functional***

Test Entity: ***VSTL***

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.

Test Method: ***Inspection***

Test Entity: ***VSTL***

2.6.3.3 Privacy

The voting system SHALL be capable of producing a paper record that does not contain any information that could link the record to the voter.

Test Method: ***Inspection***

Test Entity: ***VSTL***

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).

Test Method: ***Functional***

Test Entity: ***VSTL***

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.

Test Method: ***Inspection***

Test Entity: ***VSTL***

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.

Test Method: ***Inspection***

Test Entity: ***VSTL***

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.

Test Method: ***Inspection***

Test Entity: ***VSTL***

2.7 Performance Monitoring

2.7.1 Voting system and Network Status

2.7.1.1 Network monitoring

The voting system SHALL provide for system and network monitoring during the voting period.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.7.1.2 Tool access

The system and network monitoring functionality SHALL only be accessible to authorized personnel from restricted consoles.

Test Method: ***Functional***

Test Entity: ***VSTL***

2.7.1.3 Tool privacy

System and network monitoring functionality SHALL NOT have the capability to compromise voter privacy or election integrity.

Test Method: ***Functional***

Test Entity: ***VSTL***

Section 3: Usability

3.1 General Principles

The goal of a voting system is to have the simplest design needed to meet its intended functions. This design needs to provide guidance to the voter to assist them through the balloting process. In addition, the voting system should minimize the amount of voter inputs required to complete the balloting process.

3.2 Alternative Languages

The voting system SHALL be capable of presenting the ballot, ballot selections, review screens and instructions in any language required by state or federal law.

Test Method: Inspection

Test Entity: Manufacturer

3.3 Clarity of Instructions

The system SHALL:

a. Provide clear instructions and assistance to allow voters to successfully execute and cast their ballots independently;

b. Provide instructions for all valid operations; and

c. Clearly state the nature of the problem, when warnings and alerts are issued by the vote capture device and the set of responses available to the voter. The warning SHALL clearly state whether the voter has performed or attempted an invalid operation or whether the voting equipment itself has malfunctioned in some way.

Test Method: Inspection

Test Entity: Manufacturer

3.4 Voting Input Fields

The design of the voting input field should make it clear where and how to vote and the voting system should provide feedback that the vote was accepted by the voting system. The guidance in this section addresses these design features.

3.4.1.1 User input; voting system

The voting system shall:

a. Provide a consistent relationship between names of the candidates and where to cast a vote.

b. Clearly indicate the maximum number of candidates for whom one can vote for within a single contest; and

c. Provide sufficient computational performance in the vote capture device to provide responses to each voter entry in no more than three seconds

Test Method: ***Functional***

Test Entity: ***Manufacturer***

3.4.1.2 User input; vote capture device

The vote capture device SHALL:

a. On touch screens, provide sensitive touch areas that have a minimum height of 0.5 inches and minimum width of 0.7 inches. The vertical distance between the centers of adjacent areas shall be at least 0.6 inches, and the horizontal distance at least 0.8 inches; and

b. Provide input mechanisms designed to minimize accidental activation.

Test Method: ***Functional***

Test Entity: ***Manufacturer***

3.5 Interaction Issues

The voting process SHALL be designed to minimize interaction difficulties for the voter.

3.5.1 Navigation

3.5.1.1 Page scrolling

The vote capture device SHALL NOT require page scrolling by the voter.

Test Method: ***Functional***

Test Entity: ***Manufacturer***

3.5.1.2 Displaying contest

The vote capture device SHALL display all necessary information to cast a vote for a single contest in one place without the need to turn pages or page to other screens

Test Method: ***Functional***

Test Entity: ***Manufacturer***

3.5.1.3 Movement

The means by which voters navigate through the voting system SHALL be simple and not require complex or complicated actions (e.g., clicking on a "Next Page" button rather than scrolling).

Test Method: ***Functional***

Test Entity: ***Manufacturer***

3.5.1.4 Navigation features

Navigation features SHALL be provided that are distinct and clearly separated from voting response fields

Test Method: ***Functional***

Test Entity: ***Manufacturer***

3.5.1.5 Pace

Voters SHALL be able to control the pace and sequence of their use of the ballot. Voters SHALL be able to freely move back and forward through the ballot.

Test Method: ***Functional***

Test Entity: ***Manufacturer***

3.5.1.6 Additional time

If the vote capture device requires a response by a voter within a specific period of time, it SHALL issue an alert at least 20 seconds before this time period has expired and provide a means by which the voter may receive additional time.

Test Method: ***Functional***

Test Entity: ***Manufacturer***

3.6 Ballot Legibility

In order to facilitate usability, voting system designers should pay close attention to design elements that affect the voter's ability to clearly read and easily understand the information provided. The following guidance addresses these design features:

a. The font size and style used SHALL ensure that written material can be easily and unambiguously read.

b. Text (except labels) SHALL be presented using upper and lower case characters.

c. All text intended for the voter SHALL be presented in a sans serif font.

d. All electronic voting machines SHALL provide a minimum font size of 3.0 mm (measured as the height of a capital letter) for all text.

e. A clearly legible font SHALL be utilized. Fonts SHALL have true ascenders and descenders, uniform stroke width, and uniform aspect ratio.

f. For a given font, it SHALL be possible to clearly distinguish between the following characters: X and Y, T and Y, I and L, I and 1, O and Q, O and 0, S and 5, and U and V.

g. Instructions SHALL be concise and be designed to communicate information clearly and unambiguously so that they can be easily understood and interpreted without error.

h. Instruction steps SHALL be written in active voice as positive commands (focusing on what to do, not what not to do).

i. Punctuation SHALL conform to standard usage of the language used.

j. The use of color by the voting system SHALL agree with common conventions:

    i. Green, blue or white is used for general information or as a normal status indicator;
    ii. Amber or yellow is used to indicate warnings or a marginal status; and
    iii. Red is used to indicate error conditions or a problem requiring immediate attention.

Test Method: Functional

Test Entity: Manufacturer

3.7 Perceptual Issues

The voting system SHALL be designed to minimize perceptual difficulties for the voter.

a. No vote capture device display screen SHALL flicker with a frequency between 2 Hz and 55 Hz.

b. Any aspect of the vote capture device that is adjustable by the voter or remote voting location workers, including font size, color contrast, and audio volume, SHALL automatically reset to a standard default value upon completion of that voter's session.

c. The minimum figure-to-ground ambient contrast ratio for all text and information graphics (including icons) intended for the voter SHALL be 3:1.

Test Method: Functional

Test Entity: Manufacturer

Section 4: Software

4.1 Selection of Programming Languages

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).

Test Method: Inspection

Test Entity: Manufacturer

4.2 Selection of General Coding Conventions

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.

Test Method: Inspection

Test Entity: Manufacturer

4.2.1.1 Published

Coding conventions SHALL be considered published if they appear in publicly available media.

Test Method: Inspection

Test Entity: Manufacturer

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.3 Software Modularity and Programming

4.3.1 Modularity

Application logic SHALL be designed in a modular fashion.

4.3.1.1 Module testability

Each module SHALL have a specific function that can be tested and verified independently from the remainder of the code.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.3.1.2 Module size and identification

Modules SHALL be small and easily identifiable.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.4 Structured Programming

4.4.1 Exception Handling

4.4.1.1 Exception handling

Application logic SHALL handle exceptions using block-structured exception handling constructs.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.4.2 Unstructured Control Flow is Prohibited

Application logic SHALL contain no unstructured control constructs.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.4.2.1 Branching

Arbitrary branches (a.k.a. GoTos) SHALL NOT be allowed.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.4.2.3 Unstructured exception handling

Unstructured exception handling (e.g., On Error GoTo, setjmp/longjmp) SHALL NOT be allowed.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.5 Comments

4.5.1 Header Comments

Application logic modules SHALL include header comments that provide at least the following information for each callable unit (function, method, operation, subroutine, procedure, etc.):

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).

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.6 Executable Code and Data Integrity

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.6.2 Prevent Tampering With Code

Programmed devices SHALL defend against replacement or modification of executable or interpreted code.

Test Method: ***Inspection***

Test Entity: ***VSTL***

4.6.3 Prevent Tampering With Data

The voting system SHALL prevent access to or manipulation of configuration data, vote data, or audit records.

Test Method: ***Inspection***

Test Entity: ***VSTL***

4.7 Error Checking

4.7.1 Detect Garbage Input

4.7.1.1 Validity check

Programmed devices SHALL check information inputs for completeness and validity.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.7.1.2 Defend against garbage input

Programmed devices SHALL ensure that incomplete or invalid inputs do not lead to irreversible error.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.7.2 Mandatory Internal Error Checking

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

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 ranged-checked on every access.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.7.2.5 Garbage input parameters

All scalar or enumerated type parameters whose valid ranges as used in a callable unit (function, method, operation, subroutine, procedure, etc.) do not cover the entire ranges of their declared data types SHALL be range-checked on entry to the unit.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

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.

Test Method: ***Inspection***

Test Entity: ***VSTL***

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.

Test Method: ***Inspection***

Test Entity: ***VSTL***

4.7.2.9 Do not disable error checks

Error checks detailed in Requirement 4.7.2.1 SHALL remain active in production code.

Test Method: ***Inspection***

Test Entity: ***VSTL***

4.7.2.10 Roles authorized to respond to errors

Exceptions resulting from failed error checks or CPU-level exceptions SHALL require intervention by an election official or administrator before voting can continue.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.8 Recovery

4.8.1 Voting system Device Failure

4.8.1.1 Resuming normal operations

All voting systems SHALL be capable of resuming normal operations following the correction of a failure in any device.

Test Method: ***Functional***

Test Entity: ***Manufacturer***

4.8.1.2 Failures not compromise voting or audit data

Exceptions and system recovery SHALL be handled in a manner that protects the integrity of all recorded votes and audit log information.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

4.8.1.3 Device survive component failure

All vote capture device SHALL be capable of resuming normal operation following the correction of a failure in any component (e.g., memory, CPU, printer) provided that catastrophic electrical or mechanical damage has not occurred.

Test Method: ***Functional***

Test Entity: ***Manufacturer***

4.8.2 Controlled Recovery

Error conditions SHALL be corrected in a controlled fashion so that voting system status may be restored to the initial state existing before the error occurred.

Test Method: ***Functional***

Test Entity: ***Manufacturer***

4.8.2.1 Nested error conditions

Nested error conditions that are corrected without reset, restart, reboot, or shutdown of the vote capture device SHALL be corrected in a controlled sequence so that voting system status may be restored to the initial state existing before the first error occurred.

Test Method: ***Functional***

Test Entity: ***Manufacturer***

4.8.2.2 Reset CPU error states

CPU-level exceptions that are corrected without reset, restart, reboot, or shutdown of the vote capture device SHALL be handled in a manner that restores the CPU to a normal state and allows the voting system to log the event and recover as with a software-level exception.

Test Method: ***Functional***

Test Entity: ***Manufacturer***

4.8.3 Restore Device to Checkpoints

When recovering from non-catastrophic failure or from any error or malfunction that is within the operator's ability to correct, the voting system SHALL restore the device to the operating condition existing immediately prior to the error or failure, without loss or corruption of voting data previously stored in the device.

Test Method: ***Functional***

Test Entity: ***Manufacturer***

Section 5: Security

5.1 Access Control

This section states requirements for the identification of authorized system users, processes and devices and the authentication or verification of those identities as a prerequisite to granting access to system processes and data. It also includes requirements to limit and control access to critical system components to protect system and data integrity, availability, confidentiality, and accountability.

This section applies to all entities attempting to physically enter voting system facilities or to request services or data from the voting system.

5.1.1 Separation of Duties

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.

Test Method: ***Functional***

Test Entity: ***VSTL***

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.

Test Method: ***Functional***

Test Entity: ***VSTL***

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.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.1.2 Voting system Access

The voting system SHALL provide access control mechanisms designed to permit authorized access and to prevent unauthorized access to the system.

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.

Test Method: ***Functional***

Test Entity: ***VSTL***

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.

Test Method: ***Functional***

Test Entity: ***VSTL***

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.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.1.2.4 Escalation prevention

The voting system SHALL prevent a lower-privilege process from modifying a higher-privilege process.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.1.2.5 Operating system privileged account restriction

The voting system SHALL NOT require its execution as an operating system privileged account and SHALL NOT require the use of an operating system privileged account for its operation.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.1.2.6 Logging of account

The voting system SHALL log the identification of all personnel accessing or attempting to access the voting system to the system event log.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.1.2.7 Monitoring voting system access

The voting system SHALL provide tools for monitoring access to the system. These tools SHALL provide specific users real time display of persons accessing the system as well as reports from logs.

Test Method: Functional

Test Entity: VSTL

5.1.2.8 Login failures

Vote capture device located at the remote voting location and the central server SHALL have the capability to restrict access to the voting system after a preset number of login failures.

- The lockout threshold SHALL be configurable by appropriate administrators/operators
- The voting system SHALL log the event
- The voting system SHALL immediately send a notification to appropriate administrators/operators of the event.
- The voting system SHALL provide a mechanism for the appropriate administrators/operators to reactivate the account after appropriate confirmation.

Test Method: Functional

Test Entity: VSTL

5.1.2.9 Account lockout logging

The voting system SHALL log a notification when any account identification is locked.

Test Method: Functional

Test Entity: VSTL

5.1.2.10 Session time-out

Authenticated sessions on critical processes SHALL have an inactivity time-out control that will require personnel re-authentication when reached. This time-out SHALL be implemented for administration and monitor consoles on all voting system devices.

Test Method: Functional

Test Entity: VSTL

5.1.2.11 Screen lock

Authenticated sessions on critical processes SHALL have a screen-lock functionality that can be manually invoked.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.2 Identification and Authentication

Authentication mechanisms and their associated strength may vary from one voting system capability and architecture to another but all must meet the minimum requirement to maintain integrity and trust. It is important to consider a range of roles individuals may assume when operating different components in the voting system and each may require different authentication mechanisms.

The requirements described in this section vary from role to role. For instance, a remote voting location worker will have different identification and authentication characteristics than a voter. Also, for selected critical functions there may be cases where split knowledge or dual authorization is necessary to ensure security. This is especially relevant for critical cryptographic key management functions.

5.2.1 Authentication

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.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.2.1.2 Minimum authentication methods

The voting system SHALL authenticate users per the minimum authentication methods outlined below.

Test Method: ***Functional***

Test Entity: ***VSTL***

Table 5-1 Roles

GROUP OR ROLE	MINIMUM AUTHENTICATION STRENGTH
Election Judge	Two factor
Remote Voting Location Worker	One factor
Voter	Not required

Election Official	Two factor
Administrator	Two-factor
Application or Process	Digital signature 112 bits of security[1]

5.2.1.3 Multiple authentication mechanisms

The voting system SHALL provide multiple authentication methods to support multi-factor authentication.

Test Method: ***Functional***

Test Entity: ***VSTL***

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.

Test Method: ***Functional***

Test Entity: ***VSTL***

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.

Test Method: ***Functional***

Test Entity: ***VSTL***

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.

Test Method: ***Functional***

Test Entity: ***VSTL***

[1] NIST Special Publication 800-57 Part 1 Table 2

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.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.2.1.8 Account information password restriction

The voting system SHALL ensure that the user name is not used in the password.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.2.1.9 Automated password expiration

The voting system SHALL provide a means to automatically expire passwords.

Test Method: ***Functional***

Test Entity: ***VSTL***

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.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.2.1.11 Network authentication

Remote voting location site Virtual Private Network (VPN) connections (i.e., vote capture devices and authentication device connections) to voting servers SHALL be authenticated using strong mutual cryptographic authentication at the 112 bits of security.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.2.1.12 Message authentication

Message authentication SHALL be used for applications to protect the integrity of the message content using a schema with 112 bits of security

Test Method: ***Functional***

Test Entity: ***VSTL***

5.2.1.13 Message authentication mechanisms

IPsec, SSL, or TLS and MAC mechanisms SHALL all be configured to be compliant with FIPS 140-2 using approved algorithm suites and protocols.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.3 Cryptography

Cryptography serves several purposes in voting systems. They include:

- Confidentiality: where necessary the confidentiality of voting records can be provided by encryption;
- Authentication: data and programs can be authenticated by a digital signature or message authentication codes (MAC), or by comparison of the cryptographic hashes of programs or data with the reliably known hash values of the program or data. If the program or data are altered, then that alteration is detected when the signature or MAC is verified, or the hash on the data or program is compared to the known hash value. Typically the programs loaded on voting systems and the ballot definitions used by voting systems are verified by the systems, while systems apply digital signatures to authenticate the critical audit data that they output. For remote connections cryptographic user authentication mechanism SHALL be based on strong authentication methods; and
- Random number generation: random numbers are used for several purposes including the creation of cryptographic keys for cryptographic algorithms and methods to provide the services listed above, and as identifiers for voting records that can be used to identify or correlate the records without providing any information that could identify the voter.

5.3.1 General Cryptography Requirements

5.3.1.1 Cryptographic functionality

All cryptographic functionality SHALL be implemented using NIST-approved cryptographic algorithms/schemas, or use published and credible cryptographic algorithms/schemas/protocols.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.3.1.2 Required security strength

Cryptographic algorithms and schemes SHALL be implemented with a security strength equivalent to at least 112 bits of security to protect sensitive voting information and election records.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.3.1.3 Use NIST-approved cryptography for communications

Cryptography used to protect information in-transit over public telecommunication networks SHALL use NIST-approved algorithms and cipher suites.

Test Method: ***Function***

Test Entity: ***VSTL***

5.3.2 Key Management

The following requirements apply to voting systems that generate cryptographic keys internally.

5.3.2.1 Key generation methods

Cryptographic keys generated by the voting system SHALL use a NIST-approved key generation method, or a published and credible key generation method.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.3.2.2 Security of key generation methods

Compromising the security of the key generation method (e.g., guessing the seed value to initialize the deterministic random number generator (RNG)) SHALL require as least as many operations as determining the value of the generated key.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.3.2.3 Seed values

If a seed key is entered during the key generation process, entry of the key SHALL meet the key entry requirements see 5.3.3.1. If intermediate key generation values are output from the cryptographic module, the values SHALL be output either in encrypted form or under split knowledge procedures.

Test Method: ***Inspection***

Test Entity: ***VSTL***

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 (140-2) random number generator SHALL be used.

Test Method: ***Inspection***

Test Entity: ***VSTL***

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).

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.3.3 Key Establishment

Key establishment may be performed by automated methods (e.g., use of a public key algorithm), manual methods (use of a manually transported key loading device), or a combination of automated and manual methods.

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.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.3.4 Key Handling

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.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.3.4.2 Key zeroization

The voting system SHALL provide methods to zeroize all plaintext secret and private cryptographic keys within the system.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.3.4.3 Support for rekeying

The voting system SHALL support the capability to reset cryptographic keys to new values.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.4 Voting System Integrity Management

This section addresses the secure deployment and operation of the voting system, including the protection of removable media and protection against malicious software.

5.4.1 Protecting the Integrity of the Voting System

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.

Test Method: ***Functional***

Test Entity: ***VSTL***

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.

Test Method: ***Functional***

Test Entity: ***Manufacturer***

5.4.1.3 Cast vote storage

Cast vote data SHALL NOT be permanently stored on the voting device.

Test Method: ***Functional***

Test Entity: ***Manufacturer***

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.

Test Method: ***Functional***

Test Entity: ***Manufacturer***

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

5.4.1.6 Updating malware detection

The voting system SHALL provide a mechanism for updating malware detection signatures.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

5.5 Communications Security

This section provides requirements for communications security. These requirements address ensuring the integrity of transmitted information and protecting the voting system from external communications-based threats.

5.5.1 Data Transmission Integrity

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.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.5.1.2 TLS/SSL

Voting systems SHALL use at a minimum TLS 1.0, SSL 3.1 or equivalent protocols.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.5.1.3 Virtual private networks

Voting systems deploying VPNs SHALL configure them to only allow FIPS-compliant cryptographic algorithms and cipher suites.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.5.1.4 Unique system identifier

Each communicating device SHALL have a unique system identifier.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.5.1.5 Mutual authentication required

Each device SHALL mutually strongly authenticate using the system identifier before additional network data packets are processed.

Test Method: ***Functional***

Test Entity: ***Manufacturer***

5.5.1.6 Secrecy of ballot data

Data transmission SHALL preserve the secrecy of voters' ballot selections and SHALL prevent the violation of ballot secrecy and integrity.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.5.2 External Threats

Voting systems SHALL implement protections against external threats to which the system may be susceptible.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.5.2.1 Disabling network interfaces

Voting system components SHALL have the ability to enable or disable physical network interfaces.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.5.2.2 Minimizing interfaces

The number of active ports and associated network services and protocols SHALL be restricted to the minimum required for the voting system to function.

Test Method: ***Inspection/Vulnerability***

Test Entity: ***VSTL***

5.5.2.3 Prevention of attacks and security non-compliance

The voting system SHALL block all network connections that are not over a mutually authenticated channel.

Test Method: ***Functional/Vulnerability***

Test Entity: ***VSTL***

5.6 Logging

5.6.1 Log Management

5.6.1.1 Default settings

The voting system SHALL implement default settings for secure log management activities, including log generation, transmission, storage, analysis, and disposal.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.6.1.2 Log access

Logs SHALL only be accessible to authorized roles.

Test Method: ***Functional***

Test Entity: ***Manufacturer***

5.6.1.3 Log access

The voting system SHALL restrict log access to append-only for privileged logging processes and read-only for authorized roles.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.6.1.4 Logging events

The voting system SHALL log logging failures, log clearing, and log rotation.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.6.1.5 Log format

The voting system SHALL store log data in a publicly documented format, such as XML, or include a utility to export log data into a publicly documented format.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.6.1.6 Log separation

The voting system SHALL ensure that each jurisdiction's event logs and each component's logs are separable from each other.

Test Method: ***Functional***

Test Entity: ***Manufacturer***

5.6.1.7 Log review

The voting system SHALL include an application or program to view, analyze, and search event logs.

Test Method: ***Functional***

Test Entity: ***Manufacturer***

5.6.1.8 Log preservation

All logs SHALL be preserved in a useable manner prior to voting system decommissioning.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

5.6.1.9 Voter privacy

Logs SHALL NOT contain any data that could violate the privacy of the voter's identity.

Test Method: ***Functional***

Test Entity: ***Manufacturer***

5.6.1.10 Timekeeping format

Timekeeping mechanisms SHALL generate time and date values, including hours, minutes, and seconds.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.6.1.11 Timekeeping precision

The precision of the timekeeping mechanism SHALL be able to distinguish and properly order all log events.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.6.1.12 System clock security

Only the system administrator SHALL be permitted to set the system clock.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.6.2 Communications Logging

5.6.2.1 General

All communications actions SHALL be logged.

Test Method: ***Inspection***

Test Entity: ***VSTL***

5.6.2.2 Log content

The communications log SHALL contain at least the following entries:

- Times when the communications are activated and deactivated;
- Services accessed;
- Identification of device to which data was transmitted to or received from;
- Identification of authorized entity; and
- Successful and unsuccessful attempts to access communications or services.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.6.3 System Event Logging

This section describes requirements for the voting system to perform event logging for system maintenance troubleshooting, recording the history of system activity, and detecting unauthorized or malicious activity. The operating system, and/or applications software may perform the actual event logging. There may be multiple logs in use for any system component.

5.6.3.1 Event log format

The voting system SHALL log the following data for each event:

a. System ID;

b. Unique event ID and/or type;

c. Timestamp;

d. Success or failure of event, if applicable;

e. User ID triggering the event, if applicable; and

f. Jurisdiction, if applicable.

Test Method: Inspection

Test Entity: VSTL

5.6.3.2 Critical events

All critical events SHALL be recorded in the system event log.

Test Method: Functional

Test Entity: Manufacturer

5.6.3.3 System events

At a minimum the voting system SHALL log the events described in the table below.

Test Method: Inspection

Test Entity: Manufacturer

Table 5-2 System events

SYSTEM EVENT	DESCRIPTION
GENERAL SYSTEM FUNCTIONS	
Error and exception messages	Includes but not limited to: • The source and disposition of system interrupts resulting in entry into exception handling routines. • Messages generated by exception handlers.

SYSTEM EVENT	DESCRIPTION
	• The identification code and number of occurrences for each hardware and software error or failure. • Notification of physical violations of security. • Other exception events such as power failures, failure of critical hardware components, data transmission errors or other types of operating anomalies. • All faults and the recovery actions taken. • Error and exception messages such as ordinary timer system interrupts and normal I/O system interrupts do not need to be logged.
Critical system status messages	Critical system status messages other than information messages displayed by the device during the course of normal operations. Includes but not limited to: • Diagnostic and status messages upon startup. • The “zero totals” check conducted before opening the voting location.
Non-critical status messages	Non-critical status messages that are generated by the data quality monitor or by software and hardware condition monitors.
Events that require election official intervention	Events that require election official intervention, so that each election official access can be monitored and access sequence can be constructed.
Shutdown and restarts	Both normal and abnormal shutdowns and restarts.
Changes to system configuration settings	Configuration settings include but are not limited to registry keys, kernel settings, logging settings, and other system configuration settings.
Integrity checks for executables, configuration files, data, and logs	Integrity checks that may indicate possible tampering with files and data.
The addition and deletion of files	Files added or deleted from the system.
System readiness results	Includes but not limited to: • System pass or fail of hardware and software test for system readiness. • Identification of the software release, identification of the election to be processed, voting location identification, and the results of the software and hardware diagnostic tests. • Pass or fail of ballot style compatibility and integrity test. • Pass or fail of system test data removal.
Removable media events	Removable media that is inserted into or removed from the system.
Backup and restore	Successful and failed attempts to perform backups and restores.
Authentication related events	Includes but not limited to:

SYSTEM EVENT	DESCRIPTION
	• Login/logoff events (both successful and failed attempts). • Account lockout events. • Password changes.
Access control related events	Includes but not limited to: • Use of privileges. • Attempts to exceed privileges. • All access attempts to application and underlying system resources. • Changes to the access control configuration of the system.
User account and role (or groups) management activity	Includes but not limited to: • Addition and deletion of user accounts and roles. • User account and role suspension and reactivation. • Changes to account or role security attributes such as password length, access levels, login restrictions, permissions, etc. • Administrator account and role password resets.
Installation, upgrading, patching, or modification of software or firmware	Logging for installation, upgrading, patching, or modification of software or firmware include logging what was installed, upgraded, or modified as well as a cryptographic hash or other secure identifier of the old and new versions of the data.
Changes to configuration settings	Includes but not limited to: • Changes to critical function settings. At a minimum critical function settings include location of ballot definition file, contents of the ballot definition file, vote reporting, location of logs, and system configuration settings. • Changes to settings including but not limited to enabling and disabling services. • Starting and stopping processes.
Abnormal process exits	All abnormal process exits.
Successful and failed database connection attempts (if a database is utilized).	All database connection attempts.
Changes to cryptographic keys	At a minimum critical cryptographic settings include key addition, key removal, and re-keying.
Voting events	Includes: • Opening and closing the voting period. • Casting a vote. • Success or failure of log and election results exportation.

5.7 Incident Response

5.7.1 Incident Response Support

5.7.1.1 Critical events

Manufacturers SHALL document what types of system operations or security events (e.g., failure of critical component, detection of malicious code, unauthorized access to restricted data) are classified as critical.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

5.7.1.2 Critical event alarm

An alarm that notifies appropriate personnel SHALL be generated on the remote voting device or server, dependant upon which device has the error, if a critical event is detected.

Test Method: ***Functional***

Test Entity: ***Manufacturer***

5.8 Physical and Environmental Security

5.8.1 Physical Access

5.8.1.1 Unauthorized physical access requirement

Any unauthorized physical access SHALL leave physical evidence that an unauthorized event has taken place.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

5.8.2 Physical Ports and Access Points

5.8.2.1 Non-essential ports

The voting system SHALL disable physical ports and access points that are not essential to voting operations, testing, and auditing.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

5.8.3 Physical Port Protection

5.8.3.1 Physical port shutdown requirement

If a physical connection between the vote capture device and a component is broken, the affected vote capture device port SHALL be automatically disabled.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

5.8.3.2 Physical component alarm requirement

The voting system SHALL produce a visual alarm if a connected component is physically disconnected.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

5.8.3.3 Physical component event log requirement

An event log entry that identifies the name of the affected device SHALL be generated if a vote capture device component is disconnected.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

5.8.3.4 Physical port enablement requirement

Disabled ports SHALL only be re-enabled by authorized administrators.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

5.8.3.5 Physical port restriction requirement

Vote capture devices SHALL be designed with the capability to restrict physical access to voting machine ports that accommodate removable media with the exception of ports used to activate a voting session.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

5.8.3.6 Physical port tamper evidence requirement

Vote capture devices SHALL be designed to give a physical indication of tampering or unauthorized access to ports and all other access points, if used as described in the manufacturer's documentation.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

5.8.3.7 Physical port disabling capability requirement

Vote capture devices SHALL be designed such that physical ports can be manually disabled by an authorized administrator.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

5.8.4 Door Cover and Panel Security

5.8.4.1 Access points security requirement

Access points such as covers and panels SHALL be secured by locks or tamper evident or tamper resistance countermeasures and SHALL be implemented so that voting system owners can monitor access to vote capture devices components through these points.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

5.8.5 Secure Paper Record Receptacle

5.8.5.1 Secure paper record container requirement

If the voting system provides paper record containers then they SHALL be designed such that any unauthorized physical access results in physical evidence that an unauthorized event has taken place.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

5.8.6 Secure Physical Lock and Key

5.8.6.1 Secure physical lock access requirement

Voting equipment SHALL be designed with countermeasures that provide physical indication that unauthorized attempts have been made to access locks installed for security purposes.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

5.8.6.2 Secure locking system key requirement

Manufacturers SHALL provide locking systems for securing voting devices that can make use of keys that are unique to each owner.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

5.8.7 Media Protection

These requirements apply to all media, both paper and digital, that contain personal privacy related data or other protected or sensitive types of information.

5.8.7.1 Remote voting site protection

The voting system SHALL meet the following requirements:

a. All paper records (including rejected ones) printed at the remote voting locations SHALL be deposited in a secure container;

b. Vote capture device hardware, software and sensitive information (e.g., electoral roll) SHALL be physically protected to prevent unauthorized modification or disclosure; and

c. Vote capture device hardware components, peripherals and removable media SHALL be identified and registered by means of a unique serial number or other identifier.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

5.9 Penetration Resistance

5.9.1 Resistance to Penetration Attempts

5.9.1.1 Resistant to attempts

The voting system SHALL be resistant to attempts to penetrate the system by any remote unauthorized entity.

Test Method: ***Functional***

Test Entity: ***VSTL***

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.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.9.1.3 System access

The voting system SHALL provide no access, information or services to unauthorized entities.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.9.1.4 Interfaces

All interfaces SHALL be penetration resistant including TCP/IP, wireless, and modems from any point in the system.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.9.1.5 Documentation

The configuration and setup to attain penetration resistance SHALL be clearly and completely documented.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.9.2 Penetration Resistance Test and Evaluation

5.9.2.1 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:

- Server system;
- Vote capture devices;
- All items setup and configured per Technical Data Package (TDP) recommendations;
- Local wired and wireless networks; and
- Internet connections.

Test Method: ***Functional***

Test Entity: ***VSTL***

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 Method: ***Functional***

Test Entity: ***VSTL***

5.9.2.3 White box testing

The penetration testing team SHALL conduct white box test 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.

Test Method: ***Functional***

Test Entity: ***VSTL***

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 the ballot secrecy. The penetration testing team SHALL prioritize testing efforts based on the following:

a. Threat scenarios for the voting system under investigation;

b. Remote attacks SHALL be prioritized over in-person attacks;

c. Attacks with a large impact SHALL be prioritized over attacks with a more narrow impact; and

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.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.9.2.5 Penetration testing team establishment

The test lab SHALL establish a penetration testing team with at least two security experts. One of these experts SHALL have at least 4 years of experience in penetration testing, and the others SHALL have at least 2 years of experience.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.9.2.6 Penetration testing level of effort-test plan

In determining the level of effort to apply to penetration testing, the test lab SHALL take into consideration the size and complexity of the voting

system, any available results from the “closed end” functional, security, and usability testing activities and laboratory analysis and testing activities.

Test Method: ***Functional***

Test Entity: ***VSTL***

5.9.2.7 Penetration testing level of effort

The penetration testing team SHALL devote a minimum period of 4 staff weeks to examining and testing the voting system and to generating the reports of the testing results.

Test Method: ***Functional***

Test Entity: ***VSTL***

Section 6: Quality Assurance

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.

Test Method: Inspection

Test Entity: VSTL

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.

Test Method: Inspection

Test Entity: Manufacturer

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.

Test Method: Inspection

Test Entity: Manufacturer

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

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

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

Section 7: Configuration Management

7.1 Scope

7.1.1 Configuration Management Requirements

The configuration management documentation provided for manufacturer registration SHALL be sufficient for pilot projects.

Test Method: Inspection

Test Entity: EAC

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.

Test Method: Inspection

Test Entity: EAC

7.2 Configuration Identification

Configuration identification is the process of identifying, naming, and acquiring configuration items. Configuration identification encompasses all voting system components.

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.

Test Method: Inspection

Test Entity: Manufacturer

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.

Test Method: Inspection

Test Entity: Manufacturer

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).

Test Method: Inspection

Test Entity: Manufacturer

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).

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

7.5 Configuration Audits

7.5.1 Physical Configuration Audit

For the PCA, a manufacturer SHALL provide:

a. Identification of all items that are to be a part of the pilot voting system release;

b. Specification of compiler (or choice of compilers) to be used to generate 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 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.

Test Method: ***Inspection***

Test Entity: ***VSTL***

7.5.2 Functional Configuration Audit

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:

   i. Copies of all procedures used for module or unit testing, integration testing, and system testing;

   ii. 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

   iii. Records of all tests performed by the procedures listed above, including error corrections and retests .

Test Method: ***Functional / Inspection***

Test Entity: ***VSTL***

Section 8: Technical Data Package

8.1 Scope

This section contains a description of manufacturer documentation relating to the voting system that must be submitted with the system as a precondition of conformity assessment. These items are necessary to define the product and its method of operation; to provide technical and test data supporting the manufacturer's claims of the system's functional capabilities and performance levels; and to document instructions and procedures governing system operation and field maintenance. Any other items relevant to the system evaluation, such as media, materials, source code, object code, and sample output report formats, must be submitted along with this documentation.

This documentation is used by the VSTL in constructing the test plan. Testing of systems submitted by manufacturers that consistently adhere to particularly strong and well-documented quality assurance and configuration management practices will generally be more efficient than for systems developed and maintained using less rigorous or less well-documented practices.

Both formal documentation and notes of the manufacturer's system development process must be submitted for conformity assessment. Documentation describing the system development process permits assessment of the manufacturer's systematic efforts to develop and test the system and correct defects. Inspection of this process also enables the design of a more precise test plan. The VSTL must design and conduct the appropriate tests to cover all elements of the system and to ensure conformance with all system requirements.

8.1.1 Content and Format

The content of the Technical Data Package (TDP) is intended to provide clear, complete descriptions of the following information about the voting system:

- Overall system design, including subsystems, modules and the interfaces among them;
- Specific functional capabilities provided by the system;
- Performance and design specifications;
- Design constraints, applicable standards, and compatibility requirements;
- Personnel, equipment, and facility requirements for system operation, maintenance, and logistical support;
- Manufacturer practices for assuring system quality during the system's development and subsequent maintenance; and
- Manufacturer practices for managing the configuration of the system during development and for modifications to the system throughout its life cycle.

8.1.1.1 Required content for initial conformity assessment

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.

Test Method: Inspection

Test Entity: Manufacturer

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:

a. implementation statement;
b. The voting equipment user documentation (Section 9 “Voting Equipment User Documentation”);
c. System hardware specification;
d. Application logic design and specification;
e. System security specifications;
f. System test specification;
g. Configuration for testing; and
h. Training Documentation.

Test Method: Inspection

Test Entity: Manufacturer

8.1.1.2 Format

The requirements for formatting the TDP are general in nature; specific format details are of the manufacturer's choosing.

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.

Test Method: Inspection

Test Entity: Manufacturer

8.1.1.2.2 Cross-index

A cross-index SHALL be provided indicating the portions of the documents that are responsive to documentation requirements enumerated in section 8.1.1.1.2.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.1.2 Protection of Proprietary Information

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.2 Implementation Statement

8.2.1 TDP Implementation Statement

The TDP SHALL include an implementation statement.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.3 System Hardware Specification

8.3.1 TDP System Hardware Specification

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.3.2 System Hardware Characteristics

8.3.2.1 TDP system 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.

Test Method: Inspection

Test Entity: Manufacturer

8.3.3 Design and Construction

8.3.3.1 Identify system configuration

Manufacturers SHALL provide sufficient data, or references to data, to identify unequivocally the details of the system configuration submitted for testing.

Test Method: Inspection

Test Entity: Manufacturer

8.3.3.2 Photographs for hardware validation

Manufacturers SHALL provide photographs of the exterior and interior of devices included in the system to identify the hardware of the system configuration submitted for testing.

Test Method: Inspection

Test Entity: Manufacturer

8.3.3.3 List of materials

Manufacturers SHALL provide a list of materials and components used in the system and a description of their assembly into major system components and the system as a whole.

Test Method: Inspection

Test Entity: Manufacturer

8.3.3.4 Design and construction miscellany

Text and diagrams SHALL be provided that describe:

a. Materials, processes, and parts used in the system, their assembly, and the configuration control measures to ensure compliance with the system specification;

b. Electromagnetic environment generated by the system; and

c. Operator and voter safety considerations and any constraints on system operations or the use environment.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.3.4 Hardwired Logic

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4 Application Logic Design and Specification

8.4.1 TDP Application Logic Design and Specification

Manufacturers SHALL expand on the system overview included in the user documentation by providing detailed specifications of the application logic components of the system, including those used to support the telecommunications capabilities of the system, if applicable.

Test Method: ***Inspection***

Test Entity: Manufacturer

8.4.2 Purpose and Scope

8.4.2.1 Describe application logic functions

Manufacturers SHALL describe the function or functions that are performed by the application logic comprising the system, including that used to support the telecommunications capabilities of the system, if applicable.

Test Method: Inspection

Test Entity: Manufacturer

8.4.3 Applicable Documents

8.4.3.1 List documents controlling application logic development

Manufacturers SHALL list all documents controlling the development of application logic and its specifications.

Test Method: Inspection

Test Entity: Manufacturer

8.4.4 Application Logic Overview

8.4.4.1 Application logic overview

Manufacturers SHALL provide an overview of the application logic.

Test Method: Inspection

Test Entity: Manufacturer

8.4.4.2 Application logic architecture

The overview SHALL include a description of the architecture, the design objectives, and the logic structure and algorithms used to accomplish those objectives.

Test Method: Inspection

Test Entity: Manufacturer

8.4.4.3 Application logic design

The overview SHALL include the general design, operational considerations, and constraints influencing the design.

Test Method: Inspection

Test Entity: Manufacturer

8.4.4.4 Application logic overview miscellany

The overview SHALL include the following additional information for each separate software package:

a. Package identification;

b. General description;

c. Requirements satisfied by the package;

d. Identification of interfaces with other packages that provide data to, or receive data from, the package; and

e. Concept of execution for the package.

Test Method: Inspection

Test Entity: Manufacturer

8.4.5 Application Logic Standards and Conventions

8.4.5.1 Application logic standards and conventions

Manufacturers SHALL provide information on application logic standards and conventions developed internally by the manufacturer as well as published industry standards that have been applied by the manufacturer.

Test Method: Inspection

Test Entity: Manufacturer

8.4.5.2 Application logic standards and conventions, checklist

Manufacturers SHALL provide information that addresses the following standards and conventions related to application logic:

a. Development methodology;

b. Design standards, including internal manufacturer procedures;

c. Specification standards, including internal manufacturer procedures;

d. Coding conventions, including internal manufacturer procedures;

e. Testing and verification standards, including internal manufacturer procedures, that can assist in determining the correctness of the logic; and

f. Quality assurance standards or other documents that can be used to examine and test the application logic. These documents include standards for logic diagrams, program documentation, test planning, and test data acquisition and reporting.

Test Method: Inspection

Test Entity: ***Manufacturer***

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.6 Application Logic Operating Environment

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.7 Hardware Environment and Constraints

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.8 Application Logic Environment

8.4.8.1 Identify operating system

Manufacturers SHALL identify the operating system and the specific version thereof, or else clarify how the application logic operates without an operating system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.8.2 Identify 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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.8.3 Identify 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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.9 Application Logic Functional Specification

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.10 Functions and Operating Modes

8.4.10.1 Functions and operating modes

Manufacturers SHALL describe all application logic functions and operating modes of the system, such as ballot preparation, election programming, preparation for opening the voting period, recording votes and/or counting ballots, closing the voting period, and generating reports.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.10.2 Functions and operating modes detail

For each application logic function or operating mode, manufacturers SHALL provide:

a. A definition of the inputs to the function or mode (with characteristics, limits, tolerances or acceptable ranges, as applicable);

b. An explanation of how the inputs are processed; and

c. A definition of the outputs produced (again, with characteristics, limits, tolerances, or acceptable ranges, as applicable).

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.11 Application Logic Integrity Features

8.4.11.1 Application logic integrity features

Manufacturers SHALL describe the application logic's capabilities or methods for detecting or handling:

a. Exception conditions;

b. System failures;

c. Data input/output errors;

d. Error logging for audit record generation;

e. Production of statistical ballot data;

f. Data quality assessment; and

g. Security monitoring and control.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.12 Programming Specifications

8.4.12.1 Programming specifications

Manufacturers SHALL provide in this section an overview of the application logic's design, its structure, and implementation algorithms and detailed specifications for individual modules.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.13 Programming Specifications Overview

The programming specifications overview SHALL document the architecture of the application logic.

8.4.13.1 Programming specifications overview, diagrams

This overview SHALL include such items as UML diagrams, data flow diagrams, and/or other graphical techniques that facilitate understanding of the programming specifications.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.13.2 Internal functioning of individual modules

This section SHALL be prepared to facilitate understanding of the internal functioning of the individual modules.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.13.3 Programming specifications overview, content

Implementation of the functions SHALL be described in terms of the architecture, algorithms, and data structures.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.14 Programming Specifications Details

8.4.14.1 TDP programming specifications details

The programming specifications SHALL describe individual application logic modules and their component units, if applicable.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.14.2 Module and callable unit documentation

For each application logic module and callable unit, manufacturers SHALL document:

a. Significant module and unit design decisions, if any, such as algorithms used;

b. Any constraints, limitations, or unusual features in the design of the module or callable unit; and

c. A description of its inputs, outputs, and other data elements as applicable with respect to communication over system interfaces (see section 8.4.16 “Interfaces”).

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.14.3 Justify 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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.14.5 Source code

For each callable unit (function, method, operation, subroutine, procedure, etc.) in application logic, border logic, and third-party logic, manufacturers SHALL supply the source code.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.14.6 Inductive assertions

For each callable unit (function, method, operation, subroutine, procedure, etc.) 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 (possibly, 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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.14.7 High-level constraints

Manufacturers SHALL specify a sound argument (possibly, 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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.14.8 Safety of concurrency

Manufacturers SHALL specify a sound argument (possibly, but not necessarily, a formal proof) that application logic is free of race conditions, deadlocks, livelocks, and resource starvation.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.15 System Database

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

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).

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

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).

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

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 (alphanumeric, integer, etc.);

c. Size and format (such as length and punctuation of a character string);

d. Units of measurement (meters, seconds, etc.);

e. Range or enumeration of possible values (0–99, etc.);

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).

Test Method: Inspection

Test Entity: Manufacturer

8.4.15.6 External file maintenance and security

For external files, manufacturers SHALL document the procedures for file maintenance, management of access privileges, and security.

Test Method: Inspection

Test Entity: Manufacturer

8.4.16 Interfaces

8.4.16.1 Identify and describe interfaces

Using a combination of text and diagrams, manufacturers SHALL identify and provide a complete description of all major internal and external interfaces.

Test Method: Inspection

Test Entity: Manufacturer

8.4.17 Interface Identification

8.4.17.1 Interface identification details

For each interface identified in the system overview, manufacturers SHALL:

a. Provide a unique identifier assigned to the interface;

b. Identify the interfacing entities (systems, configuration items, users, etc.) by name, number, version, and documentation references, as applicable; and

c. Identify which entities have fixed interface characteristics (and therefore impose interface requirements on interfacing entities) and which are being developed or modified (thus having interface requirements imposed upon them).

Test Method: Inspection

Test Entity: Manufacturer

8.4.18 Interface Description

8.4.18.1 Interface types

For each interface identified in the system overview, manufacturers SHALL describe the type of interface (e.g., real-time data transfer or data storage-and-retrieval) to be implemented.

Test Method: Inspection

Test Entity: Manufacturer

8.4.18.2 Interface signatures

For each interface identified in the system overview, manufacturers SHALL describe characteristics of individual data elements that the interfacing entity(ies) will provide, store, send, access, receive, etc., such as:

a. Names/identifiers;

b. Data type (alphanumeric, integer, etc.);

c. Size and format (such as length and punctuation of a character string);

d. Units of measurement (meters, seconds, etc.);

e. Range or enumeration of possible values (0–99, etc.);

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).

Test Method: Inspection

Test Entity: Manufacturer

8.4.18.3 Interface protocols

For each interface identified in the system overview, manufacturers SHALL describe characteristics of communication methods that the interfacing entity(ies) will use for the interface, such as:

a. Communication links/bands/frequencies/media and their characteristics;

b. Message formatting;

c. Flow control (e.g., sequence numbering and buffer allocation);

d. Data transfer rate, whether periodic/aperiodic, and interval between transfers;

e. Routing, addressing, and naming conventions;

f. Transmission services, including priority and grade; and

g. Safety/security/privacy considerations, such as encryption, user authentication, compartmentalization, and auditing.

Test Method: Inspection

Test Entity: Manufacturer

8.4.18.4 Protocol details

For each interface identified in the system overview, manufacturers SHALL describe characteristics of protocols the interfacing entity(ies) will use for the interface, such as:

a. Priority/layer of the protocol;

b. Packeting, including fragmentation and reassembly, routing, and addressing;

c. Legality checks, error control, and recovery procedures;

d. Synchronization, including connection establishment, maintenance, termination; and

e. Status, identification, and any other reporting features.

Test Method: Inspection

Test Entity: Manufacturer

8.4.18.5 Characteristics of interfaces

For each interface identified in the system overview, manufacturers SHALL describe any other pertinent characteristics, such as physical compatibility of the interfacing entity(ies) (dimensions, tolerances, loads, voltages, plug compatibility, etc.).

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.4.19 Appendices

Manufacturers SHALL provide descriptive material and data supplementing the various sections of the body of the logic specifications. The content and arrangement of appendices are at the discretion of the manufacturer. Topics recommended for amplification or treatment in appendix form include:

- Glossary: A listing and brief definition of all module names and variable names, with reference to their locations in the logic structure. Abbreviations, acronyms, and terms should be included, if they are either uncommon in data processing and software development or are used with an unorthodox meaning;
- References: A list of references to all related manufacturer documents, data, standards, and technical sources used in logic development and testing; and
- Program Analysis: The results of logic configuration analysis algorithm analysis and selection, timing studies, and hardware interface studies that are reflected in the final logic design and coding.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5 System Security Specifications

This section defines the documentation requirements for systems. These recommendations apply to the full scope of system functionality, including functionality for defining the ballot and other pre-voting functions, as well as functions for casting and storing votes, vote reporting, system logging, and maintenance of the system. User documentation includes all public information that is provided to end users. The Technical Data Package (TDP) includes the user documentation along with proprietary information that is viewed only by the VSTL.

8.5.1 General

8.5.1.1 Overall security

Manufacturers SHALL document in the TDP all aspects of system design, development, and proper usage that are relevant to system security. This includes, but is not limited to the following:

- System security objectives;
- All hardware and software security mechanisms;
- All cryptographic algorithms, protocols and schemes that are used;

- Development procedures employed to ensure absence of malicious code;
- Initialization, usage, and maintenance procedures necessary to secure operation;
- All attacks the system is designed to resist or detect; and
- Any security vulnerabilities known to the manufacturer.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.1.2 High level security

Manufacturers SHALL provide at a minimum the high-level documents listed in Table 8-1 as part of the TDP.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

Table 8-1 High level system documentation

DOCUMENT	DESCRIPTION
Security Threats Controls	This document identifies the threats the system protects against and the implemented security controls on system and system components.
Security Architecture	This document provides an architecture level description of how the security requirements are met, and SHALL include the various authentication, access control, audit, confidentiality, integrity, and availability requirements.
Interface Specification	This document describes external interfaces (programmatic, human, and network) provided by each of the computer components of the system.
Design Specification	This document provides a high-level design of each system component.
Development Environment Specification	This document provides descriptions of the physical, personnel, procedural, and technical security of the development environment including configuration management, tools used, coding standards used, software engineering model used, and description of developer and independent testing.
Security Testing and Vulnerability Analysis Documentation	This document describes security tests performed to identify vulnerabilities and the results of the testing. This also includes testing performed as part of software development, such as unit, module, and subsystem testing.

8.5.2 Access Control

8.5.2.1 General user

Manufacturers SHALL provide user and TDP documentation of access control capabilities of the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.2.2 General access control technical specification

Manufacturers SHALL provide descriptions and specifications of all access control mechanisms of the system including management capabilities of authentication, authorization, and passwords in the TDP.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.2.3 Unauthorized access technical specification

Manufacturers SHALL provide descriptions and specifications of methods to prevent unauthorized access to the access control mechanisms of the system in the TDP.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.2.4 Access control dependent system mechanisms

Manufacturers SHALL provide descriptions and specifications of all system mechanisms that are dependent upon, support, and interface with access controls in the TDP.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.2.5 Voting operations and roles

Manufacturers SHALL provide a list of all of the operations possible on the voting system and list the default roles that have permission to perform each such operation as part of the TDP.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.2.6 Critical event escalation

Manufacturers SHALL document a prioritized critical event escalation list of appropriate personnel to be notified.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.3 System Event Logging

8.5.3.1 General

Manufacturers SHALL provide TDP documentation of event logging capabilities of the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.4 Software Installation

8.5.4.1 Software list technical data package

Manufacturers SHALL provide a list of all software related to the system in the technical data package (TDP).

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.4.2 Software information

Manufacturers SHALL provide, at a minimum in the TDP, the following information for each piece of software related to the system:

- Software product name;
- Software version number;
- Software manufacturer name;
- Software manufacturer contact information;
- Type of software (application logic, border logic, third party logic, COTS software, or installation software);
- List of software documentation;
- Component identifier(s) (such as filename(s)) of the software; and
- Type of software component (executable code, source code, or data).

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.4.3 Software location information

Manufacturers SHALL provide the location (such as full path name or memory address) and storage device (such as type and part number of storage device) where each piece of software is installed on programmed devices of the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.4.4 Software functionality for programmed devices

Manufacturers SHALL document the functionality provided to the system by the software installed on programmed devices.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.4.5 Software dependencies and interaction

Manufacturers SHALL map the dependencies and interactions between software installed on programmed devices.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.4.6 Build environment software and hardware

Manufacturers SHALL provide a list of all software and hardware required to assemble the build environment used to create system software executable code including application logic, border logic, and third party logic.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.4.7 Build environment assembly procedures

Manufacturers SHALL document the procedures to assemble the build environment(s) used to create system software executable code including application logic, border logic, and third party logic.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.4.8 System software build procedures

Manufacturers SHALL document the procedures used to build the system software executable code including application logic, border logic, and third party logic.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.5 Physical Security

8.5.5.1 Unauthorized physical access

Manufacturers SHALL provide a list of all system components to which access must be restricted and a description of the function of each said component.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.5.2 Physical port and access point

Manufacturers SHALL provide a listing of all ports and access points.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.5.3 Physical lock documentation of use

For each lock, manufacturers SHALL document whether the lock was installed to secure an access point.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.5.4 Power usage

Manufacturer SHALL provide a list of all physical security countermeasures that require power supplies.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.5.5 Physical security

Manufacturer SHALL document the design and implementation of all physical security controls for the system and its components.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.6 System Integrity Management

8.5.6.1 Binaries per system

Manufacturers SHALL provide a list of the binaries that are required to be executed on the system devices.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.7 Setup Inspection

8.5.7.1 Software integrity verification

Manufacturers SHALL provide a technical specification of how the integrity of software installed on programmed devices of the system is verified.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.7.2 Software integrity verification technique software non-modification

Manufacturers SHALL provide documentation of software integrity verification techniques that prevent the modification of software installed on programmed devices of the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.7.3 Register and variable value inspection

Manufacturers SHALL provide a technical specification of how the inspection of all the system registers and variables is implemented by the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.7.4 Backup power inspection

Manufacturers SHALL provide a technical specification of how the inspection of the remaining charge of the backup power sources is implemented by the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.7.5 Cabling connectivity inspection

Manufacturers SHALL provide a technical specification of how the inspection of the connectivity of cabling attached is implemented by the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.7.6 Communications operational status inspection

Manufacturers SHALL provide a technical specification of how the inspection of the operational status of the communications capability is implemented by the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.7.7 Communications on/off inspection

Manufacturers SHALL provide a technical specification of how the inspection of the on/off status of the communications capability is implemented by the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.7.8 Consumable inspection

Manufacturers SHALL provide a technical specification of how the inspection of the remaining amount of each consumable is implemented by the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.7.9 Calibration of voting device components inspection

Manufacturers SHALL provide a technical specification of how the inspection of the calibration for each component is implemented by the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.5.7.10 Calibration of voting device components adjustment

Manufacturers SHALL provide a technical specification of how the adjustment to the calibration of each component is implemented by the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.6 System Test Specification

Manufacturers SHALL provide test specifications for:

a. Development test specifications; and

b. System test specifications.

Test Method: Inspection

Test Entity: Manufacturer

8.6.1 Development Test Specifications

8.6.1.1 Development test specifications

Manufacturers SHALL describe the plans, procedures, and data used during development and system integration to verify system logic correctness, data quality, and security. This description SHALL include:

a. Test identification and design, including test structure, test sequence or progression, and test conditions;

b. Standard test procedures, including any assumptions or constraints;

c. Special purpose test procedures including any assumptions or constraints;

d. Test data, including the data source, whether it is real or simulated, and how test data are controlled;

e. Expected test results; and

f. Criteria for evaluating test results.

Test Method: Inspection

Test Entity: Manufacturer

8.6.2 System Test Specifications

RFI 2007-03 contains several requirements for usability testing by the manufacturer and that each of these requirements also mandates that the manufacturer report the test results as part of the TDP. These requirements are not present in this section but need to be considered as part of the system test specifications.

8.6.2.1 Specifications for verification and validation of system performance

Manufacturers SHALL provide specifications for verification and validation of overall system performance. These specifications SHALL cover:

a. Control and data input/output;

b. Processing accuracy;

c. Data quality assessment and maintenance;

d. ballot interpretation logic;

e. Exception handling;

f. Security;

g. Production of audit trails and statistical data;

h. Expected test results; and

i. Criteria for evaluating test results.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.6.2.2 Demonstrate fitness for purpose

The specifications SHALL identify procedures for assessing and demonstrating the suitability of the system for election use.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.7 Configuration for Testing

8.7.1 Configuration Description

Configuration of hardware and software, both operating systems and applications, is critical to proper system functioning. Correct test design and sufficient test execution must account for the intended and proper configuration of all system components. If the system can be set up in both conforming and nonconforming configurations, the configuration actions necessary to obtain conforming behavior must be specified.

8.7.1.1 Hardware set-up

Manufacturers SHALL provide instructions and photographs illustrating the proper set-up of the system hardware.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.7.1.2 Provide answers to installation prompts

Manufacturers SHALL provide a record of all user selections that must be made during software/firmware installation for the system to meet the requirements of the UOCAVA Pilot Testing Requirements.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

8.7.1.3 Configuration data

Manufacturers SHALL submit all configuration data needed to set up and operate the system.

Test Method: ***Inspection***

Test Entity: Manufacturer

Section 9: System Users Manual

9.1 Scope

This section contains requirements on the content of the documentation that manufacturers supply to jurisdictions that use their systems. In this context, "user" refers to election officials, others in the jurisdiction who implement systems, and VSTLs. The user documentation is also included in the TDP provided to the VSTL.

It is not the intent of these requirements to prescribe an outline for user documentation. Manufacturers are encouraged to innovate in the quality and clarity of their user documentation. The intent of these requirements is to ensure that certain information that is of interest to end users and VSTLs will be included within the user documentation. To expedite the VSTL review, manufacturers SHALL provide the VSTL with a short index that relates the corresponding sections of the user documentation to the specific requirements in this document.

9.2 System Overview

9.2.1 User Documentation System Overview

In the system overview, manufacturers SHALL provide information that enables the user to identify the functional and physical components of the system, how the components are structured, and the interfaces between them.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.2.2 System Overview Functional Diagram

The system overview SHALL include a high-level functional diagram of the system that includes all of its components. The diagram SHALL portray how the various components relate and interact.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.2.3 System Description

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 (dial-up, 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.

Test Method: Inspection

Test Entity: Manufacturer

9.2.3.2 Identify software and firmware by origin

The system description SHALL include the identification of all software and firmware items, indicating items that were:

a. Written in-house;

b. Written by a subcontractor;

c. Procured as COTS; and

d. Procured and modified, including descriptions of the modifications to the software or firmware and to the default configuration options.

Test Method: Inspection

Test Entity: Manufacturer

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.

Test Method: Inspection

Test Entity: Manufacturer

9.2.4 System Performance

9.2.4.1 User documentation system performance

Manufacturers SHALL provide system performance information including:

a. Device capacities and limits that were stated in the implementation statement;

b. Performance characteristics of each operating mode and function in terms of expected and maximum speed, throughput capacity, maximum volume (maximum number of voting positions and maximum number of ballot styles supported), and processing frequency;

c. Quality attributes such as reliability, maintainability, availability, usability, and portability;

d. Provisions for safety, security, voter privacy, ballot secrecy, and continuity of operations; and

e. Design constraints, applicable standards, and compatibility requirements.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.3 System Functionality Description

9.3.1 User Documentation, System Functionality Description

Manufacturers SHALL provide a listing of the system's functional processing capabilities, encompassing capabilities required by the UOCAVA Pilot Testing Requirements, and any additional capabilities provided by the system, with a description of each capability.

a. Manufacturers SHALL explain, in a manner that is understandable to users, the capabilities of the system declared in the implementation statement;

b. Additional capabilities (extensions) SHALL be clearly indicated;

c. Required capabilities that may be bypassed or deactivated during installation or operation by the user SHALL be clearly indicated;

d. Additional capabilities that function only when activated during installation or operation by the user SHALL be clearly indicated; and

e. Additional capabilities that normally are active but may be bypassed or deactivated during installation or operation by the user SHALL be clearly indicated.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.4 System Security Specification

9.4.1 Access Control

9.4.1.1 Access control implementation, configuration, and management

Manufacturers SHALL provide user documentation containing guidelines and usage instructions on implementing, configuring, and managing access control capabilities.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.4.1.3 Privileged account

Manufacturers SHALL disclose and document information on all privileged accounts included on the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.4.2 System Event Logging

9.4.2.1 System event logging

Manufacturers SHALL provide user documentation that describes system event logging capabilities and usage.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.4.2.2 Log format

Manufacturers SHALL provide fully documented log format information.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.4.3 Ballot Decryption

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.4.4 Physical Security

9.4.4.1 Physical security

Manufacturers SHALL provide user documentation explaining the implementation of all physical security controls for the system, including procedures necessary for effective use of countermeasures.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.4.5 Audit

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.4.5.2 Machine readability of paper record

Manufacturers SHALL provide documentation for a procedure to scan the paper record by optical character recognition.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.5 Software

9.5.1 Software installation

9.5.1.1 Software list

Manufacturers SHALL provide a list of all software to be installed on the programmed devices of the system and installation software used to install the software.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.5.1.2 Software information

Manufacturers SHALL provide at a minimum, the following information for each piece of software to be installed or used to install software on programmed devices of the system: software product name, software version number, software manufacturer name, software manufacturer contact information, type of software (application logic, border logic, third party logic, COTS software, or installation software), list of software documentation, component identifier(s) (such filename(s)) of the software, type of software component (executable code, source code, or data).

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.5.1.3 Software location information

Manufacturers SHALL provide the location (such as full path name or memory address) and storage device (such as type and part number of storage device) where each piece of software is installed on programmed devices of the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.5.1.4 Election specific software identification

Manufacturers SHALL identify election specific software in the user documentation.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.5.1.5 Installation software and hardware

Manufacturers SHALL provide a list of software and hardware required to install software on programmed devices of the system in the user documentation.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.5.1.6 Software installation procedure

Manufacturers SHALL document the software installation procedures used to install software on programmed devices of the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

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.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.5.1.8 Procurement of system software

The software installation procedures SHALL specify that system software SHALL be obtained from the VSTL or approved distribution repositories.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.5.1.9 Open market procurement of COTS software

The software installation procedures SHALL specify that COTS software SHALL be obtained from the open market.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.5.1.10 Erasable storage media preparation

The software installation procedures SHALL specify how previously stored information on erasable storage media is removed before installing software on the media.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.5.1.11 Installation media unalterable storage media

The software installation procedures SHALL specify that unalterable storage media SHALL be used to install software on programmed devices of the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.5.1.12 Software hardening

Manufacturers SHALL provide documentation that describes the hardening procedures for the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6 Setup Inspection

9.6.1 Setup inspection process

Manufacturers SHALL provide a setup inspection process that the system was designed to support.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.1 Minimum properties included in a setup inspection process

A setup inspection process SHALL, at a minimum, include the inspection of system software, storage locations that hold election information that

changes during an election, other voting device properties, and execution of logic and accuracy testing related to readiness for use in an election.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.2 Setup inspection record generation

The setup inspection process SHALL describe the records that result from performing the setup inspection process.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.3 Installed software identification procedure

Manufacturers SHALL provide the procedures to identify all software installed on programmed devices.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.4 Software integrity verification procedure

Manufacturers SHALL describe the procedures to verify the integrity of software installed on programmed devices of system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.5 Election information value

Manufacturers SHALL provide the values of system storage locations that hold election information that changes during the election, except for the values set to conduct a specific election.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.6 Maximum values of election information storage locations

Manufacturers SHALL provide the maximum values for the storage locations that the election information resides in.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.7 Register and variable value inspection procedure

Manufacturers SHALL provide the procedures to inspect the values of voting device storage locations that hold election information that changes for an election.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.8 Backup power operational range

Manufacturers SHALL provide the nominal operational range for the backup power sources of the voting device.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.9 Backup power inspection procedure

Manufacturers SHALL provide the procedures to inspect the remaining charge of the backup power sources of the voting device.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.10 Cabling connectivity inspection procedure

Manufacturers SHALL provide the procedures to inspect the connectivity of the cabling attached to the voting device.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.11 Communications operational status inspection procedure

Manufacturers SHALL provide the procedures to inspect the operational status of the communications capabilities of the voting device.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.12 Communications on/off status inspection procedure

Manufacturers SHALL provide the procedures to inspect the on/off status of the communications capabilities of the voting device.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.13 Consumables quantity of voting equipment

Manufacturers SHALL provide a list of consumables associated with the voting device, including estimated number of usages per quantity of consumable.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.14 Consumable inspection procedure

Manufacturers SHALL provide the procedures to inspect the remaining amount of each consumable of the voting device.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.15 Calibration of voting device components nominal range

Manufacturers SHALL provide a list of components associated with the voting device that require calibration and the nominal operating ranges for each component.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.16 Calibration of voting device components inspection procedure

Manufacturers SHALL provide the procedures to inspect the calibration of each component.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.17 Calibration of voting device components adjustment procedure

Manufacturers SHALL provide the procedures to adjust the calibration of each component.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.6.1.18 Checklist of properties to be inspected

Manufacturers SHALL provide a checklist of other properties of the system to be inspected.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7 System Operations Manual

9.7.1 General

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 remote voting locations, with regard to all system functions and operations identified in Section 9.3 System Functionality Description.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

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 remote voting site workers.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.2 Introduction

9.7.2.1 Functions

Manufacturers SHALL provide a summary of system operating functions to permit understanding of the system's capabilities and constraints.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.2.2 Roles

The roles of operating personnel SHALL be identified and related to the functions of the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.2.3 Conditional actions

Decision criteria and conditional operator functions (such as error and failure recovery actions) SHALL be described.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.2.4 References

Manufacturers SHALL list all reference and supporting documents pertaining to the use of the system during election operations.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.3 Operational Environment

9.7.3.1 Operational environment

Manufacturers SHALL describe the system environment and the interfaces between the system and State and/or local election officials, remote voting site workers, system administrators, and voters.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.3.2 Operational environment; equipment and facility

Manufacturers SHALL identify all facilities, furnishings, fixtures, and utilities that will be required for equipment operations, including equipment that operates at the:

a. Remote voting location;

b. State and/or local election offices; and

c. Other locations.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.3.3 Operational environment; installation

The operations manual SHALL include a statement of all requirements and restrictions regarding environmental protection, electrical service, recommended auxiliary power, telecommunications service, and any other facility or resource required for the proper installation and operation of the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.4 System Installation and Test Specification

9.7.4.1 Readiness testing

Manufacturers SHALL provide specifications for testing of system installation and readiness.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.4.1.1 Readiness test entire system

These specifications SHALL cover testing of all components of the system and all locations of installation (e.g., remote voting locations, state and/or local election offices), and SHALL address all elements of system functionality and operations identified in Section 9.3 System Functionality Description above, including general capabilities and functions specific to particular voting activities.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.5 Operational Features

9.7.5.1 Features

Manufacturers SHALL provide documentation of system operating features that includes:

a. Detailed descriptions of all input, output, control, and display features accessible to the operator or voter;

b. Examples of simulated interactions to facilitate understanding of the system and its capabilities;

c. Sample data formats and output reports; and

d. Illustration and description of all status indicators and information messages.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.5.2 Document straight party override algorithms

For systems that support straight party voting, manufacturers SHALL document the available algorithms for counting straight party overrides.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.5.3 Document double vote reconciliation algorithms

For systems that support write-in voting, manufacturers SHALL document the available algorithms for reconciling write-in double votes.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.6 Operating Procedures

9.7.6.1 Operating procedures

Manufacturers SHALL provide documentation of system operating procedures that:

a. Provides a detailed description of procedures required to initiate, control, and verify proper system operation;

b. Enables the operator to assess the correct flow of system functions (as evidenced by system-generated status and information messages);

c. Enables the administrator to intervene in system operations to recover from an abnormal system state;

d. Defines and illustrates the procedures and system prompts for situations where operator intervention is required to load, initialize, and start the system;

e. Defines and illustrates procedures to enable and control the external interface to the system operating environment if supporting hardware and software are involved. Such information also SHALL be provided for the interaction of the system with other data processing systems or data interchange protocols;

f. Provides administrative procedures and off-line operator duties (if any) if they relate to the initiation or termination of system operations, to the assessment of system status, or to the development of an audit trail;

g. Supports successful ballot and program installation and control by state and/or local election officials;

h. Provides a schedule and steps for the software and ballot installation, including a table outlining the key dates, events and deliverables; and

i. Specifies diagnostic tests that may be employed to identify problems in the system, verify the correction of problems, and isolate and diagnose faults from various system states.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.6.2 Printer error recovery guidelines

Manufacturers SHALL provide documentation for procedures to recover from printer errors and faults including procedures for how to cancel a vote suspended during an error.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.7 Transportation and Storage

9.7.7.1 Transportation

Manufacturers SHALL include any special instructions for preparing voting devices for shipment.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.7.2 Storage

Manufacturers SHALL include any special storage instructions for voting devices.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.7.3 Precautions for removable media

Manufacturers SHALL detail the care and handling precautions necessary for removable media and records.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.7.8 Appendices

Manufacturers SHALL provide descriptive material and data supplementing the various sections of the body of the system operations manual. The content and arrangement of appendices are at the discretion of the manufacturer. Topics required for discussion include:

- Glossary: A listing and brief definition of all terms that may be unfamiliar to persons not trained in either systems or computer operations;
- References: A list of references to all manufacturer documents and to other sources related to operation of the system;
- Detailed Examples: Detailed scenarios that outline correct system responses to faulty operator input; and

- Manufacturer's Recommended Security Procedures: Security procedures that are to be executed by the system operator.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.8 System Maintenance Manual

9.8.1.1 User documentation system maintenance manual

The system maintenance manual SHALL provide information to support election workers, information systems personnel, or maintenance personnel in the adjustment or removal and replacement of components or modules in the field.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.8.1.2 General contents

Manufacturers SHALL describe service actions recommended to correct malfunctions or problems; personnel and expertise required to repair and maintain the system, equipment, and materials; and facilities needed for proper maintenance.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.8.2 Introduction

9.8.2.1 Equipment overview, maintenance viewpoint

Manufacturers SHALL describe the structure and function of the hardware, firmware and software for election preparation, programming, vote recording, tabulation, and reporting in sufficient detail to provide an overview of the system for maintenance and for identification of faulty hardware or software.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.8.3 Maintenance Procedures

9.8.3.1 Maintenance manual maintenance procedures

Manufacturers SHALL describe preventive and corrective maintenance procedures for hardware, firmware and software.

Test Method: ***Inspection***

Test Entity: Manufacturer

9.8.3.2 Maintenance manual preventive maintenance procedures

Manufacturers SHALL identify and describe:

a. All required and recommended preventive maintenance tasks, including software and data backup, database performance analysis, and database tuning;

b. Number and skill levels of personnel required for each task;

c. Parts, supplies, special maintenance equipment, software tools, or other resources needed for maintenance; and

d. Any maintenance tasks that must be referred to the manufacturer.

Test Method: Inspection

Test Entity: Manufacturer

9.8.3.3 Corrective maintenance procedures

9.8.3.3.1 Troubleshooting procedures

Manufacturers SHALL provide fault detection, fault isolation, correction procedures, and logic diagrams for all operational abnormalities identified by design analysis and operating experience.

Test Method: Inspection

Test Entity: Manufacturer

9.8.3.3.2 Troubleshooting procedures details

Manufacturers SHALL identify specific procedures to be used in diagnosing and correcting problems in the system hardware, firmware and software. Descriptions SHALL include:

a. Steps to replace failed or deficient equipment;

b. Steps to correct deficiencies or faulty operations in software or firmware;

c. Number and skill levels of personnel needed to accomplish each procedure;

d. Special maintenance equipment, parts, supplies, or other resources needed to accomplish each procedure; and

e. Any coordination required with the manufacturer.

Test Method: Inspection

Test Entity: Manufacturer

9.8.4 Maintenance Equipment

9.8.4.1 Special equipment

Manufacturers SHALL identify and describe any special purpose test or maintenance equipment recommended for fault isolation and diagnostic purposes.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.8.5 Parts and Materials

Manufacturers SHALL provide detailed documentation of parts and materials needed to operate and maintain the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.8.6 Maintenance Facilities and Support

9.8.6.1 Maintenance environment

Manufacturers SHALL identify all facilities, furnishings, fixtures, and utilities that will be required for equipment maintenance.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.8.6.2 Maintenance support and spares

Manufacturers SHALL specify:

a. Recommended number and locations of spare devices or components to be kept on hand for repair purposes during periods of system operation;

b. Recommended number and locations of qualified maintenance personnel who need to be available to support repair calls during system operation; and

c. Organizational affiliation (e.g., jurisdiction, manufacturer) of qualified maintenance personnel.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.8.7 Appendices

Manufacturers SHALL provide descriptive material and data supplementing the various sections of the body of the system maintenance manual. The content and arrangement of appendices are at the discretion of the manufacturer. Topics required for amplification or treatment in the appendix include:

- Glossary: A listing and brief definition of all terms that may be unfamiliar to persons not trained in either systems or computer maintenance;
- References: A list of references to all manufacturer documents and other sources related to maintenance of the system;
- Detailed Examples: Detailed scenarios that outline correct system responses to faulty operator input; and
- Maintenance and Security Procedures: Technical illustrations and schematic representations of electronic circuits unique to the system.

Test Method: Inspection

Test Entity: Manufacturer

9.9 Personnel Deployment and Training Requirements

Manufacturers SHALL describe the personnel resources and training required for a jurisdiction to operate and maintain the system for the duration of the pilot project.

Test Method: Inspection

Test Entity: Manufacturer

9.9.1 Personnel

9.9.1.1 Training manual personnel

Manufacturers SHALL specify the number of personnel and skill levels required to perform each of the following functions:

a. Pre-voting or election preparation functions;
b. System operations for system functions performed at the remote voting locations;
c. System operations for system functions performed at the State and/or local election office;
d. Preventive maintenance tasks;
e. Diagnosis of faulty hardware, firmware, or software;
f. Corrective maintenance tasks; and
g. Testing to verify the correction of problems.

Test Method: Inspection

Test Entity: ***Manufacturer***

9.9.1.2 User functions versus manufacturer functions

Manufacturers SHALL distinguish which functions may be carried out by user personnel and which must be performed by manufacturer personnel.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

9.9.2 Training

9.9.2.1 Training requirements

Manufacturers SHALL provide training materials to instruct system administrators, remote voting location workers, and state and/or local election officials on how to set up, configure and operate the system.

Test Method: ***Inspection***

Test Entity: ***Manufacturer***

Appendix A: Definitions of Words with Special Meanings

This section of the Pilot Program Requirements defines words (terms) that are used in the other parts of the Pilot Program Requirements, particularly in requirements text.

NOTE: Readers may already be familiar with definitions for many of the words in this section, but the definitions here often may differ in small or big ways from locality usage because they are used in special ways in the Pilot Program Requirements.

Terminology for standardization purposes must be sufficiently precise and formal to avoid ambiguity in the interpretation and testing of the standard. Terms must be defined to mean exactly what is intended in the requirements of the standard, no more and no less. Consequently, this terminology may differ from common election and plain English usage, and may be unsuitable for applications that are beyond the scope of the Pilot Program Requirements. Readers are especially cautioned to avoid comparisons between this terminology and the terminology used in election law.

Any term that is defined neither in this terminology standard nor in any of the referenced documents has its regular (i.e., dictionary) meaning.

Each term is followed by a normative definition.

absentee ballot:	A ballot cast from any location not defined as a polling place.
absentee model:	The ballot remains associated with the voter ID and is subject to an adjudication process to be accepted.
absentee voting:	The process of casting a ballot from any location not defined as a polling place.
administrator:	The role responsible for installing, configuring, and managing the technical operations of the system.
application logic:	Software, firmware, or hardwired logic from any source that is specific to the system, with the exception of border logic.
audit:	Systematic, independent, documented process for obtaining records, statements of fact or other relevant information and assessing them objectively to determine the extent to which specified requirements are fulfilled
authenticated session:	Process that requires all users to provide proof of identity.
ballot image:	Human-readable electronic representation of the ballot, including the voter's selections.
ballot question:	Contest in which the choices are Yes and No.
ballot secrecy:	Not being able to associate the selections of the ballot with the voter who cast it.
ballot style:	Particular set of contests to appear on the ballot for a particular election district, their order, the list of ballot positions for each contest, and the binding of candidate names to ballot positions
ballot:	The official presentation of all of the contests to be decided in a particular election. See also ballot image, cast vote record, and paper record.

baseline configuration:	The exact system configuration tested by the VSTL. It includes all the system components that were tested, including the specific hardware, operating system, application software, and third-party COTS applications.
border logic:	Software, firmware, or hardwired logic that is developed to connect application logic to COTS or third-party logic.
callable unit:	Function, method, operation, subroutine, procedure, or analogous structural unit that appears within a module (of a software program or analogous logical design).
candidate:	Person contending in a contest for office.
cast ballot:	Ballot in which the voter has taken final action in the selection of contest choices and which has been accepted.
cast vote record:	The record of all votes selected by a voter.
CIF:	Common Industry Format
common industry format:	Format described in ISO/IEC 25062:2006 "Common Industry Format (CIF) for Usability Test Reports".
component:	A discrete and identifiable element of hardware or software within a system.
concept of operations:	Description of roles and responsibilities for system administration, operation and use.
configuration data:	Non-executable input to software, firmware, or hardwired logic, not including vote data.
conformity assessment:	Demonstration that specified requirements relating to a product, process, system, person or body are fulfilled.
contest:	A single decision being put before the voters (e.g., the selection of candidates or the response to ballot questions).
core logic:	Subset of application logic that is responsible for vote recording and tabulation.
COTS:	Commercial Off the Shelf
credible:	Methodologies (e.g., coding conventions, cryptographic algorithms) are 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.
CVR:	Cast vote record
device:	Functional unit that performs its assigned tasks as an integrated whole.
election definition:	Definition of the contests and questions that will appear on the ballot for a specific election.
election judge:	In this sense, an official on the canvassing board that adjudicates the acceptance of absentee ballots
election management system:	Set of processing functions and databases within a system that defines, develops and maintains election databases, performs election definitions and setup functions, format ballots, count votes, consolidates and report results, and maintains audit trails
election official:	The people associated with administering and conducting elections.
election title:	The heading on a ballot specifying the name of the election (e.g., General Election, Primary Election).

equivalent configuration:	A system configuration that has been attested to by the manufacturer to perform identically to the baseline configuration.
error rate:	Ratio of the number of errors detected in relation to the volume of data processed:
failure:	Events that result in (a) loss of one or more functions, (b) degradation of performance such that the device is unable to perform its intended function for longer than 10 seconds, (c) automatic reset, restart or reboot of the voting device, operating system or application software, (d) a requirement for an unanticipated intervention by a person in the role of poll worker or technician before normal operation can continue, or (e) error messages and/or audit log entries indicating that a failure has occurred.
fault:	Flaw in design or implementation that may result in the qualities or behavior of the system deviating from the qualities or behavior that are specified in the Pilot Program Testing Requirements and/or in manufacturer-provided documentation.
hardwired logic:	Logic implemented through the design of an integrated circuit; the programming of a Programmable Logic Device (PLD), Field-Programmable Gate Array (FPGA), Peripheral Interface Controller (PIC), or similar; the integration of smaller hardware components; or mechanical design (e.g., as in lever machines).
implementation statement:	Statement by a manufacturer indicating the capabilities, features, and optional functions and extensions that have been implemented in a system.
inspection:	Examination of a product design, product, process or installation and determination of its conformity with specific requirements or, on the basis of professional judgment, with general requirements.
manufacturer:	Entity with ownership and control over a system submitted for testing.
module:	Structural unit of software or analogous logical design, typically containing several callable units that are tightly coupled.
paper record identifier:	Unique randomly generated code that links the paper record to the corresponding cast vote record.
paper record receptacle:	A secure unit for storing paper records at remote voting locations.
paper record:	Printed record of selections made by the voter.
programmed device:	Electronic device that includes application logic.
published:	Methodologies (e.g., coding conventions, cryptographic algorithms) are considered published if they appear in publicly available media.
remote voting location workers:	Election workers who staff the remote voting locations.
remote voting location:	Locations at which absentee voting takes place.
straight party override:	Ability to make an exception to straight party voting in selected races.
straight party voting:	Mechanism that allows voters to cast a single vote to select all candidates on the ballot from a single political party.
summative usability testing:	Evaluation of a product with representative users and tasks designed to measure the usability (defined as effectiveness, efficiency and satisfaction) of the complete product.

test:	Technical operation that consists of the determination of one or more characteristics of a given product, process or service according to a specified procedure.
third-party logic:	Software, firmware, or hardwired logic that is neither application logic nor COTS; e.g., general-purpose software developed by a third party that is either customized (e.g., ported to a new platform, as is Windows CE) or not widely used, or source code generated by a COTS package.
UOCAVA:	Uniformed and Overseas Citizens Absentee Voting Act
vote capture device:	Device that is used directly by a voter to vote a ballot.
voted ballot:	Ballot that contains all of a voter's selections and has been cast
voter privacy:	The inability of anyone to observe, or otherwise determine, what selections a voter has made.
voting process:	Entire array of procedures, people, resources, equipment and locations associated with the conduct of elections.
voting session:	Span of time beginning when a ballot is enabled or activated and ending when that ballot cast.
voting system:	Equipment (including hardware, firmware, and software), materials, and documentation used to define elections and ballot styles, configure voting equipment, identify and validate voting equipment configurations, perform readiness tests, activate ballots, capture votes, count votes, generate reports, transmit election data, archive election data, and audit elections.
VPN:	Virtual Private Network
VSTL:	Voting System Test Laboratory
white-box:	Uses an internal perspective of the system to design test cases based on internal structure. White box testing strategy deals with the internal logic and structure of the code.
write-in:	To make a selection of an individual not listed on the ballot.

Appendix B: List of References

The following is a list of documents or publications used in the creation of the UOCAVA Pilot Program Requirements

ANSI 02:	ANSI/TIA-968-A: 2002, Technical Requirements for Connection of Terminal Equipment to the Telephone Network.
BS 7799:	Data center certification standard
CERT 06:	CERT® Coordination Center, Secure Coding homepage, July 2006, Available from http://www.cert.org/secure-coding/.
DHS 06:	Department of Homeland Security, Build Security In, July 2006, Available from https://buildsecurityin.us-cert.gov/.
EAC06:	U.S. Election Assistance Commission, Testing and Certification Program Manual, Version 1.0, December 5, 2006. Available from http://www.eac.gov/program-areas/voting-systems/docs/testingandcertmanual.pdf/attachment_download/file.
FIPS 81:	(1980): DES Modes of Operation
FIPS 46-3:	(1999): Data Encryption Standard (DES)
FIPS 140-2:	Security Requirements for Cryptographic Modules
FIPS 180-2:	(2002): Secure Hash Standard (SHA1)
FIPS 186-2:	(2000): Digital Signature Standard (DSS)
FIPS 197:	(2001): Advanced Encryption Standard (AES)
FIPS 198:	(2002): The Keyed-Hash Message Authentication Code (HMAC)
FIPS 200:	Minimum security requirements for federal information and information systems.
FCC 07a:	Title 47, Part 68, Rules and Regulations of the Federal Communications Commission, Connection of Terminal Equipment to the Telephone Network: 2000.
GPO 90:	Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems, January 1990 edition with April 1990 revisions, in Voting System Standards, U.S. Government Printing Office, 1990.14 Available from http://josephhall.org/fec_vss_1990_pdf/1990_VSS.pdf.
GPO 99:	Government Paper Specification Standards No. 11, February 1999.
HAVA 02:	The Help America Vote Act of 2002, Public Law 107-252. Available from http://www.fec.gov/hava/hava.htm.
HFP 07:	Human Factors and Privacy Subcommittee of the TGDC, "Usability Performance Benchmarks for the VVSG," August 2007. Available from http://vote.nist.gov/meeting-08172007/Usability-Benchmarks-081707.pdf.
IEEE 00:	IEEE 100:2000 The Authoritative Dictionary of IEEE Standard Terms, Seventh Edition.

IEEE 97:	IEEE/EIA 12207.1-1997, Industry implementation of International Standard ISO/IEC 12207:1995—(ISO/IEC 12207) standard for information technology—software life cycle processes—life cycle data.
IEEE 98:	IEEE Std 829-1998, IEEE standard for software test documentation.
IETF RFC 2246:	(1999): The TLS Protocol Version 1.0
IETF RFC 2510:	(1999): Internet X.509 PKI Certificate Management Protocols
IETF RFC 2817:	(2000): Upgrading to TLS within HTTP/1.1
IETF RFC 2818:	(2000): HTTP Over TLS
IETF RFC 3280:	(1999): Internet X.509 PKI Certificate and CRL Profile
IETF RFC 3369:	(2002): Cryptographic Message Syntax
IETF RFC 3370:	(2002): Cryptographic Message Syntax (CMS) Algorithms
IETF RFC 3546:	(2003): TLS Extensions
IETF RFC 3739:	(2004): Internet X.509 PKI Qualified Certificates Profile
IETF RFC 4279:	(2005): Pre-Shared Key Cipher suites for TLS
ISO 00:	ISO 9001:2000, Quality management systems – Requirements.
ISO 00a:	ISO/IEC TR 15942:2000, Information technology—Programming languages—Guide for the use of the Ada programming language in high integrity systems.
ISO 03:	ISO 10007:2003, Quality management systems – Guidelines for configuration management.
ISO 03a:	ISO/IEC 14882:2003, Programming languages—C.
ISO 04a:	ISO 17000:2004, Conformity assessment—Vocabulary and general principles.
ISO 05:	ISO 9000:2005, Quality management systems – Fundamentals and vocabulary.
ISO 06:	ISO/IEC 23270:2006, Information technology—Programming languages—C#.
ISO 06e:	ISO/IEC 25062:2006 Common Industry Format (CIF) for Usability Test Reports.
ISO 94:	ISO 9706:1994, Information and documentation—Paper for documents—Requirements for permanence.
ISO 95:	ISO/IEC 8652:1995, Information technology—Programming languages—Ada.
ISO 98a:	ISO 9241-11:1998, Ergonomic requirements for office work with visual display terminals (VDTs) -- Part 11: Guidance on usability.
ISO 99:	ISO/IEC 9899:1999, Programming languages—C.
ITU-T X.509:	(2000)/ISO/IEC 9594-8 (2001): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework
Java 05:	The Java Language Specification, Third Edition, 2005. Available from http://java.sun.com/docs/books/jls/index.html.
LOTSE-V:	Legal, Operational and Technical Standards for E-Voting

MIL 83:	MIL-STD-810-D, Environmental Test Methods and Engineering Guidelines, 1983-7-19.
MIL 85:	MIL-STD-1521B (USAF) Technical Reviews and Audits for Systems, Equipments [sic], and Computer Software, rev. December 19, 1985.
MIL 96:	MIL-HDBK-781A, Handbook for Reliability Test Methods, Plans, and Environments for Engineering, Development, Qualification, and Production, April 1, 1996.
MIRA 04:	MISRA-C:2004: Guidelines for the use of the C language in critical systems, MIRA Limited, U.K., November 2004.
Morris 84:	F. L. Morris and C. B. Jones, "An Early Program Proof by Alan Turing," IEEE Annals of the History of Computing, v. 6, n. 2, April 1984, pp. 139-143.
Moulding 89:	M. R. Moulding, "Designing for high integrity: the software fault tolerance approach," Section 3.4. In C. T. Sennett, ed., High-Integrity Software, Plenum Press, New York and London, 1989.
MS 05:	Request For Proposal #3443, Mississippi, April 28, 2005.
MS 05:	Paul Vick, The Microsoft® Visual Basic® Language Specification, Version 8.0, 2005. Available from Microsoft Download Center, http://go.microsoft.com/fwlink/?linkid=62990.
NGC 06:	Nevada Gaming Commission and State Gaming Control Board, Technical Standards for Gaming Devices and On-Line Slot Systems, March 2006. Available from http://gaming.nv.gov/stats_regs/reg14_tech_stnds.pdf.
NIST 02:	John P. Wack, Ken Cutler, Jamie Pole, National Institute of Standards and Technology Special Publication 800-41: Guidelines on Firewalls and Firewall Policy, January 2002. Available from http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf.
NIST 03:	Fred R. Byers, Care and Handling of CDs and DVDs—A Guide for Librarians and Archivists, National Institute of Standards and Technology Special Publication 500-252, 2003-10. Available from http://www.itl.nist.gov/div895/carefordisc/index.html.
NIST 05:	Recommended Security Controls for Federal Information Systems, National Institute of Standards and Technology Special Publication 800-53, 2005-02. Available from http://csrc.nist.gov/publications/nistpubs/.
NIST 05a:	Peter Mell, Karen Kent, Joseph Nusbaum, National Institute of Standards and Technology Special Publication 800-83: Guide to Malware Incident Prevention and Handling, November 2005. Available from http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf.
NIST 07:	Karen Scarfone, Peter Mell, National Institute of Standards and Technology Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems, February 2007. Available from http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf.
NIST 75:	Saltman, Roy, National Institute of Standards Special Publication 500-30, Effective Use of Computing Technology in Vote-Tallying, 1975. Available from http://csrc.nist.gov/publications/nistpubs/NBS_SP_500-30.pdf.
ODBP CR:	ODBP Code Review
ODBP CRM:	ODBP Certification Matrix
ODBP DSF:	ODBP Description of System Features
ODBP P:	ODBP Plan

ODBP SPV:	ODBP System Performance Validation
ODBP SR:	ODBP System Requirements
ODBP SM:	ODBP Security Requirements Mapped to VVSG 2005
ODBP TR:	ODBP Test Report
OMG 07:	OMG Unified Modeling Language Superstructure Specification, version 2.1.1. Document formal/2007-02-05, Object Management Group, February 2007. Available from http://www.omg.org/cgi-bin/doc?formal/2007-02-05.
Oxford 93:	New Shorter Oxford English Dictionary, Clarendon Press, Oxford, 1993.
Pietrek 97:	Matt Pietrek, "A Crash Course on the Depths of Win32™ Structured Exception Handling," Microsoft Systems Journal, January 1997. Available from http://www.microsoft.com/msj/0197/exception/exception.aspx.
PKCS #1:	RSA Cryptography Standard
PKCS #5:	Password-based Encryption Standard
PKCS #7:	Cryptographic Message Syntax Standard
PKCS #8:	Private Key Information Syntax Standard
PKCS #10:	Certification Request Standard
PKCS #11:	Cryptographic Token Interface
PKCS #12:	Personal Information Exchange Syntax Standard
SCAM 01:	Joel Scambray, Stuart McClure, George Kurtz, Hacking Exposed: Network Security Secrets and Solutions, Second Edition, 2001.
SERVE DSF:	SERVE Description of System Features
SERVE EV:	SERVE Election Validation
SERVE R:	SERVE Requirements
SERVE SA:	SERVE Security Architecture
SERVE SACP:	SERVE System Accreditation and Certification Process
SERVE STC:	SERVE Security Test Conditions
SERVE TDP C:	SERVE TDP Checklist
SERVE TRA:	SERVE Threat Risk Assessment
SERVE VVP:	SERVE Vote Verification Process
SERVE WH:	SERVE White Hat
Sourceforge 00:	CEXCEPT (exception handling in C), software package, 2000. Available from http://cexcept.sourceforge.net/.
SP 800-53:	Rev 2 Recommended Security Controls for Federal Information Systems

SP 800-63:	Electronic Authentication Guideline, April 2006. Available from: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.
SP 800-113:	(2007): DRAFT Guide to SSL VPNs
TRIVS RN:	Testing Requirements for Internet Voting Systems Robert Naegele
UL 05:	UL 60950-1:2005, Information Technology Equipment – Safety – Part 1: General Requirements.
UL 437:	UL 437:2003, Standard for Key Locks. (2003).
UOCAVA PT:	UOCAVA Penetration Testing
UT 04:	Solicitation #DG5502, Utah, 2004-07-09. January 27, 2006.
VOI CAR:	VOI Certification and Accreditation Report
VOI COD:	VOI Concepts of Operations
VOI DSF:	VOI Description of System Features
VOI LEO M:	VOI LEO Manual
VOI LEO SSRS:	VOI LEO Server Software Requirement Spec
VOI PPR:	VOI Pilot Peer Review
VOI PSR:	VOI Pilot System Requirements
VOI Report:	VOI Test Report 2001
VOI SA:	VOI System Arch
VOI SD:	VOI System Design
VOI SP:	VOI Security Policy
VOI SRS:	VOI Software Requirement Spec
VOI STEP:	VOI System Test and Evaluation Plan
VOI STP:	VOI Software Test Plan
VOI TP:	VOI Test Procedures
VOI TR:	VOI Test Report 1999
VSS 2002:	2002 Voting Systems Standards. Available from http://www.eac.gov/program-areas/voting-systems/docs/voting-systems-standards-volume-i-performance.pdf/attachment_download/file
VVSG 2005:	2005 Voluntary Voting System Guidelines, Version 1.0, March 6, 2006. Available from http://www.eac.gov/program-areas/voting-systems/docs/vvsgvolumei.pdf/attachment_download/file
VVSG 2.0:	VVSG Recommendations to the EAC, TGDC, August 31, 2007.
RFI 2007-03:	EAC Decision on Request for Interpretation 2007-03, 2005 VVSG Vol. 1 Section 3.1.1,

	September 5, 2007. Available from http://www.eac.gov/program-areas/voting-systems/docs/certification-docs-eac-decision-on-request-for-interpretation-2007-03.pdf-1/attachment_download/file.
Wald 47:	Abraham Wald, Sequential Analysis, John Wiley & Sons, 1947.

Appendix C: Accuracy Test Case

Some voting system performance attributes are tested by inducing an event or series of events, and the relative or absolute time intervals between repetitions of the event has no significance. Although equivalence between a number of events and a time period can be established when the operating scenarios of a system can be determined with precision, another type of test is required when such equivalence cannot be established. It uses eventbased failure frequencies to arrive at ACCEPT/REJECT criteria. This test may be performed simultaneously with time-based tests.

For example, the failure of a device is usually dependent on the processing volume that it is required to perform. The elapsed time over which a certain number of actuation cycles occur is, under most circumstances, not important. Another example of such an attribute is the frequency of errors in reading, recording, and processing vote data.

The error frequency, called “ballot position error rate,” applies to such functions as process of detecting the presence or absence of a voting punch or mark, or to the closure of a switch corresponding to the selection of a candidate.

Certification and acceptance test procedures that accommodate event-based failures are, therefore, based on a discrete, rather than a continuous probability distribution. A Probability Ratio Sequential Test using the binomial distribution is recommended. In the case of ballot position error rate, the calculation for a specific device (and the processing function that relies on that device) is based on:

- HO: Desired error rate = 1 in 10,000,000
- H1: Maximum acceptable error rate = 1 in 500,000
- a = 0.05
- b = 0.05

and the minimum error-free sample size to accept for qualification tests is 1,549,703 votes.

The nature of the problem may be illustrated by the following example, using the criteria contained in the *Guidelines* for system error rate. A target for the desired accuracy is established at a very low error rate. A threshold for the worst error rate that can be accepted is then fixed at a somewhat higher error rate. Next, the decision risk is chosen, that is, the risk that the test results may not be a true indicator of either the system's acceptability or unacceptability. The process is as follows:

- The desired accuracy of the voting system, whatever its true error rate (which may be far better), is established as no more than one error in every ten million characters (including the null character)
- If it can be shown that the system's true error rate does not exceed one in every five hundred thousand votes counted, it will be considered acceptable. This is more than accurate enough to declare the winner correctly in almost every election

- A decision risk of 5 percent is chosen, to be 95 percent sure that the test data will not indicate that the system is bad when it is good or good when it is bad

This results in the following decision criteria:

a. If the system makes one error before counting 26,997 consecutive ballot positions correctly, it will be rejected. The vendor is then required to improve the system

b. If the system reads at least 1,549,703 consecutive ballot positions correctly, it will be accepted

c. If the system correctly reads more than 26,997 ballot positions but less than 1,549,703 when the first error occurs, the testing will have to be continued until another 1,576,701 consecutive ballot positions are counted without error (a total of 3,126,404 with one error)

Attachment F – 04.23.2010 EAC Request Letter to Federal Voting Assistance Program

U. S. ELECTION ASSISTANCE COMMISSION
OFFICE OF THE EXECUTIVE DIRECTOR
1225 New York Avenue, NW, Suite 1100
Washington, DC. 20005

April 23, 2010

Bob Carey, Director
Federal Voting Assistance Program (FVAP)
Department of Defense
1155 Defense Pentagon
Washington, DC 20301-1155

Sent via mail and email

Dear Mr. Carey,

As the EAC finalizes the work on UOCAVA Pilot Voting System Requirements, we would like to reiterate our appreciation to you and your staff for all of your hard work in assisting with that project. We also look forward to working closely with FVAP as the EAC and NIST move forward to develop the remote electronic absentee voting guidelines for UOCAVA voters that will allow FVAP to develop a remote electronic voting system as required by section 1604(a) of the 2002 and section 567 of the 2005 National Defense Authorization Acts.

As we begin the important effort of developing guidelines for remote electronic absentee voting, the EAC and NIST need to be acutely aware of the specific security needs of FVAP for such a voting system. The EAC views FVAP not only as a partner in this effort, but as a customer who must be satisfied that the product developed by the EAC and NIST will be useful in your system design efforts. The need for improved customer satisfaction resonated with us after reviewing your public comment to our Draft Pilot Program Requirements document. This comment expressed concern about the level of security in that document being significantly less than FVAP desires for UOCAVA pilot systems.

EAC understands that FVAP has stated that the risk level has already been decided in a de facto manner as a level of risk equal to that accepted by the current absentee voting system. As the system developers, EAC requests that FVAP define the specific security assurance level it desires for a remote electronic voting system to serve UOCAVA voters. This level of risk should be stated at a level of specificity sufficient to allow us to develop testable security guidelines for electronic absentee voting systems. This policy decision will provide the framework for EAC and NIST to create and adopt final guidelines and ultimately allow FVAP to better serve the needs of its voters through the design and implementation of its remote electronic voting system.

Sincerely,

Thomas R. Wilkey

Attachment G – Draft NISTIR 7682, Information System Security Best Practices for UOCAVA – Supporting Systems (out for public comment)

Draft NISTIR 7682

Information System Security Best Practices for UOCAVA-Supporting Systems

Geoff Beier
Santosh Chokhani
Nelson Hastings
Jim Knoke
Andrew Regenscheid
Scott Shorter

National Institute of Standards and Technology
U.S. Department of Commerce

[This page intentionally left blank.]

Draft NISTIR 7682

Information System Security Best Practices for UOCAVA-Supporting Systems

Geoff Beier
Santosh Chokhani
Nelson Hastings
Jim Knoke
Andrew Regenscheid
Scott Shorter

April 2010

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director

[This page intentionally left blank.]

Acknowledgements

The authors, Andrew Regenscheid and Nelson Hastings of NIST, and Geoff Beier, Santosh Chokhani, Jim Knoke, and Scott Shorter of CygnaCom, wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content. In particular, the authors would like to acknowledge Shirley Radack, Ray Perlner, Erika McCallister, Murugiah Souppaya, Karen Scarfone, and John Wack of NIST, Matt Masterson, and James Long of the Election Assistance Commission, and Carol Paquette, Mark Skall and Tom Caddy for their feedback on drafts of this document.

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Electronic mail: uocava-voting@nist.gov

Table of Contents

EXECUTIVE SUMMARY **1**

1 INTRODUCTION **3**

1.1 PURPOSE AND SCOPE 3
1.2 INTENDED AUDIENCE 4

2 GENERAL OVERVIEW **5**

2.1 OVERSEAS VOTING SYSTEMS COMPONENTS 5
2.2 TECHNICAL CONTROLS 6
2.3 OPERATIONAL CONTROLS 7
2.4 ASSURANCE CONTROLS 7

3 SECURITY CONTROLS **9**

3.1 IDENTIFICATION AND AUTHENTICATION (I&A) 9
3.1.1 Threats to Credential Issuance Methods and Mitigations *9*
3.1.2 Credential Issuance Methods *10*
3.1.3 Threats to Authentication Mechanisms and Mitigations *10*
3.1.4 Threats to Authentication Protocols and Mitigations *11*
3.1.5 Types of Authentication Mechanisms *12*
3.1.5.1 Token Based Authentication 12
3.1.5.2 Biometric Authentication 16
3.1.6 Best Practices for Voting Systems *16*
3.2 ACCESS CONTROL 17
3.2.1 Types of Access Control *17*
3.2.1.1 Discretionary Access Control (DAC) 17
3.2.1.2 Role Based Access Control (RBAC) 18
3.2.1.3 Privilege/Attribute Based Access Control (PBAC/ABAC) 18
3.2.1.4 Mandatory Access Control (MAC) 18
3.2.1.5 Type Enforcement 18
3.2.1.6 Capability Based Access Control (CBAC) 18
3.2.2 Threats to Access Control Mechanisms *19*
3.2.3 Best Practices for Voting Systems *19*
3.3 PERSONALLY IDENTIFIABLE INFORMATION (PII) PROTECTION 19
3.3.1 Personally Identifiable Information (PII) *20*
3.3.2 Threats to PII *20*
3.3.3 Best Practices for Protection of PII in Transit *22*
3.3.4 Best Practices for Protection of PII in Storage *22*
3.4 CONFIDENTIALITY 23
3.4.1 Information Requiring Confidentiality Protection *23*
3.4.2 Best Practices for Confidentiality Protection of Information in Transit *23*
3.4.3 Best Practices for Confidentiality Protection of Information in Storage *24*
3.5 INTEGRITY 24
3.5.1 Information Requiring Integrity Protection *25*
3.5.2 Best Practices for Integrity Protection of Information in Transit *26*
3.5.3 Best Practices for Integrity Protection of Information in Storage *26*
3.6 AVAILABILITY 27
3.6.1 System Data Backup *27*
3.6.2 System Redundancy *28*
3.6.3 Best Practices for Availability of Functions *29*
3.7 CRYPTOGRAPHIC SECURITY 29
3.7.1 Certification Authority (CA) Requirements *29*
3.7.2 Certificate Checking *30*
3.7.3 Cryptographic Algorithms *30*
3.7.4 Cryptographic Module Engineering *30*
3.7.5 Best Practices for Managing Cryptographic Keys *31*
3.8 COMMUNICATION SYSTEMS 31
3.8.1 Email *31*

3.8.2 Fax and Telephone PBX *32*

4 VOTING SYSTEM NETWORK PROTECTIONS **34**

4.1 FIREWALL 34
4.1.1 Firewall Types *34*
4.1.1.1 Packet Filtering Firewall 34
4.1.1.2 Stateful Inspection Firewall 35
4.1.1.3 Application-Proxy Gateways 35
4.1.1.4 Circuit-Level Gateways 36
4.1.1.5 Dedicated Proxy Servers 36
4.1.2 Best Practices for Voting Systems *37*
4.2 INTRUSION DETECTION SYSTEM 37
4.2.1 IDS/IPS Detection Methods *38*
4.2.1.1 Signature-based Detection 38
4.2.1.2 Anomaly-based Detection 38
4.2.1.3 Stateful Protocol Analysis 39
4.2.2 IDS/IPS Technologies *39*
4.2.2.1 Network-based 39
4.2.2.2 Network Behavior Analysis (NBA) 39
4.2.2.3 Host-based IDS/IPS 39
4.2.3 Components of IDS/IPS *40*
4.2.4 IDS/IPS Functions *40*
4.2.5 Securing IDS/IPS *40*
4.2.6 Best Practices for IDS/IPS for Voting Systems *40*
4.3 VIRTUAL PRIVATE NETWORK (VPN) 41
4.3.1 Gateway-to-Gateway *42*
4.3.2 Host-to-Gateway *42*
4.3.3 Host-to-Host VPN *42*
4.4 LOG MANAGEMENT INFRASTRUCTURE 42
4.5 BEST PRACTICES FOR VOTING SYSTEM: NETWORK ARCHITECTURE 43

5 HOST PROTECTION **45**

5.1 OPERATING SYSTEM IDENTIFICATION & AUTHENTICATION (I&A) 45
5.2 OPERATING SYSTEM DISCRETIONARY ACCESS CONTROL 45
5.3 ACCOUNT MANAGEMENT 45
5.4 EVENT LOG 45
5.5 HOST-BASED FIREWALL 46
5.6 MINIMIZE SERVICES 46
5.7 HOST BASED INTRUSION DETECTION AND PREVENTION 47
5.8 MALWARE PROTECTION 47
5.9 BACKUP AND RESTORE 47
5.10 VOTING SYSTEM APPLICATION SECURITY 47
5.10.1 Application Level Identification & Authentication *48*
5.10.2 Application Discretionary Access Control *48*
5.10.3 Application Account Management *48*
5.10.4 Application Event Log *48*
5.10.5 General Application Security Practices *49*
5.10.6 Web Application Security Practices *49*
5.11 WORKSTATION NETWORK PROTECTIONS 50
5.11.1 Firewall *50*
5.11.2 Intrusion Detection System *50*
5.11.3 Virtual Private Network *50*

6 OPERATIONAL CONTROLS **51**

6.1 FACILITY CONTROLS 51
6.2 MEDIA STORAGE AND OFF-SITE BACKUP 51
6.3 PERSONNEL SECURITY CONTROLS 51
6.3.1 Position Categorization *51*
6.3.2 Separation of Duties *51*

6.3.3 Qualifications, Experience, and Training *51*
6.4 EVENT LOG PROCESSING 52
6.4.1 Frequency of Event Log Processing *52*
6.4.2 Frequency of Event Log Review *52*
6.4.3 Vulnerability Assessments *52*
6.5 BACKUP AND ARCHIVE 53
6.6 CONFIGURATION MANAGEMENT 53
6.6.1 Baseline Configuration *53*
6.6.2 Configuration Change Control *53*
6.6.3 System Hardware and Software Inventory *53*
6.6.4 Cryptographic Material inventory *53*
6.7 DISASTER RECOVERY 54
6.8 ONGOING TESTING 54
6.8.1 Penetration Testing *54*
6.8.2 Network Configuration Monitoring *54*
6.8.3 Availability Monitoring and Load Testing *54*
6.8.4 Compliance Audit *54*
6.9 INCIDENT HANDLING 55
6.10 REMOVAL FROM SERVICE 55

7 ASSURANCE REQUIREMENTS 56

7.1 DOCUMENTATION REQUIREMENTS 56
7.1.1 Administration Guidance *56*
7.1.1.1 Secure Delivery, Installation, and Start-up Guides 56
7.1.1.2 Administration Guide 57
7.1.1.3 Maintenance, Upgrade, and Flaw Remediation Procedures 57
7.1.2 Design Documents *57*
7.2 VULNERABILITY ANALYSIS 58
7.3 TESTING REQUIREMENTS 58

8 REFERENCES 59

8.1 DOCUMENTS AND PAPERS 59
8.2 USEFUL WEBSITES 60

9 LIST OF ACRONYMS 61

10 GLOSSARY 64

Executive Summary

The *Uniformed and Overseas Citizens Absentee Voting Act* (UOCAVA) protects the absentee voting rights for U.S. Citizens, including active members of the uniformed services and the merchant marines, and their spouses and dependents who are away from their place of legal voting residence. It also protects the voting rights of U.S. civilians living overseas. Federal, state and local election administrators are charged with ensuring that each UOCAVA voter can exercise the right to vote. In order to meet this responsibility, election officials must provide assorted mechanisms that enable overseas voters to obtain information about voter registration and voting procedure descriptions, and to receive and return their ballots. UOCAVA also establishes requirements for reporting statistics on the effectiveness these mechanisms to the Election Assistance Commission.

In order to streamline the process of absentee voting and to ensure that these voters are not adversely impacted by the transit delays involved due to the difficulty of mail delivery around the world, Information Technology (IT) systems can be used to facilitate overseas absentee voting in several ways. They can:

- Distribute information about the process of applying for absentee ballots, including eligibility requirements and application forms.
- Distribute information about the facts relating to specific elections, including dates, offices involved and the text of ballot questions.
- Collect completed voter registration applications.
- Inform voters of their registration status.
- Provide ballot tracking information.
- Distribute blank ballots.
- Collect voted ballots.
- Maintain statistics used to prepare the UOCAVA-mandated reports.
- Maintain absentee voter registration information used to distribute ballots.

IT systems used to provide these functions face a variety of threats. If IT systems are not selected, configured and managed using security practices commensurate with the importance of the services they provide and the sensitivity of the data they handle, a security compromise could carry severe consequences for the integrity of the election, or the confidentiality of sensitive voter information. Failure to adequately address threats to these systems could prevent voters from casting ballots, expose individuals to identity fraud, or even compromise the results of an election. This document offers procedural and technical guidance, along with references to additional resources, to assist jurisdictions with the secure deployment of these systems. The guidance found in this document focuses on IT systems used to support overseas remote voting but does not define a specific architecture or configuration.

Component and system selection guidance

The technical controls outlined in this document rely on features that are frequently, but not always, found in commercially available IT products. In some cases, a product may appear to offer a feature but fail to support the options required for secure operation. Many of the practices required for secure operation are relevant to both IT systems as a whole and to the individual discrete components that may be used to build these systems. As a result, it is important that organizations or individuals responsible for selecting the IT products that will be deployed understand these controls and the features required to implement them both in the case of purchasing a turn-key system or selecting components to assemble into a system.

Care should be taken to ensure that IT products selected offer sufficient capabilities to be integrated and deployed as part of a UOCAVA voting system with the controls described in this document. The functionality and adequacy of these capabilities should be evaluated by a neutral third party or by the agency acquiring the products.

Component and system configuration guidance

In most cases, the IT products used to support overseas absentee voting will be general-purpose commercial products suitable for a wide variety of applications with widely differing security requirements. As such, these products will be

highly configurable. Many of the options offered by these products are not appropriate for every application, and could result in a security posture that is insufficient for a critical system or for one that contains sensitive data.

The guidelines in this document aim to assist system designers and administrators in two ways. First, as systems and components are configured for operation, this document lists sets of controls and configuration options that are critical to system security. When creating configuration checklists for systems which will support voting, every type of control should be addressed for every component where it can be applied. Second, this document details options for security controls which jurisdictions can use to help meet their security objectives for voting applications. The configuration practices found in this document aim to ensure that selections appropriate to the criticality and sensitivity of the systems are made, and address all security-critical facets of configuration. Depending on the architecture or implementation of the overseas remote voting system, jurisdictions will have customized their configurations.

Operational Guidance

Finally, both technical and procedural controls are critical to securing these systems in operation. Organizations operating IT systems in support of UOCAVA voting should have comprehensively-documented, detailed security procedures for bringing the systems to a secure operating state, maintaining that secure state during operation, and securely terminating operations.

The guidance in this publication will assist election officials in collaborating with system designers and administrators to define roles and establish processes that ensure the ongoing secure operation of the systems. It should also be consulted by system designers when documenting system operations and by administrators when assigning individuals to fulfill roles defined by the system design.

1 Introduction

To support State and local election officials in carrying out their responsibilities under the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), the Election Assistance Commission (EAC) requested that the National Institute of Standards and Technology (NIST) research electronic technologies that could facilitate the UOCAVA voting process. A number of state and local jurisdictions have begun to use information technology (IT) systems and the Internet to facilitate UOCAVA voting. These systems have been, and are being, used to distribute election information to voters, to send and collect voter registration and ballot request forms, to deliver blank ballots, and to receive voted ballots. This document is intended to provide jurisdictions with a set of computer security best practices that can be used as a baseline set of controls for securing their IT systems, and the supporting infrastructure. It examines the large collection of cyber security resources, including standards, guidelines, tools, and metrics, that NIST has developed to help federal agencies under the Federal Information Security Management Act (FISMA) of 2002 and summarizes them for those designing, deploying, or using information technology systems that support UOCAVA voting.

In December 2008, NIST released NISTIR 7551, *A Threat Analysis on UOCAVA Voting Systems* [NISTIR7551], which documents the threats to UOCAVA voting systems using electronic technologies for all aspects of the overseas voting process. NISTIR 7551 identified a number of threats to using electronic technologies to obtain voter registration materials, deliver blank ballots, or return cast ballots, emphasizing the need for implementing strong and comprehensive security controls to mitigate the identified threats. While NISTIR 7551 discussed high-level security controls capable of mitigating threats, the focus of that report was identifying technologies and associated risks. This document complements NIST 7551 by providing detailed security best practices to help jurisdictions obtain, deploy, manage and use UOCAVA voting systems based on security practices used in other IT applications.

At the time of the release of this draft, the EAC has posted a draft of their *UOCAVA Pilot Program Testing Requirements* document [PILOTREQ]. The *UOCAVA Pilot Program Testing Requirements* document defines conformance requirements for remote electronic voting systems using a manned-kiosk architecture that is intended for use in a UOCAVA pilot program. Nothing in this document should be construed to supersede any requirements provided in the EAC's *UOCAVA Pilot Program Testing Requirements* document. The scope of this document is much broader than the UOCAVA pilot program thus some of the best practices described in this document may not be suitable for the specific pilot architecture.

1.1 Purpose and Scope

This document provides best practices for the secure operation of information systems that support overseas voting in accordance with the requirements of the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) [HAVA, UOCAVA]. These best practices are based on existing NIST standards and guidelines used to secure non-national security information systems. This document summarizes the standards and guidelines that were deemed most applicable for jurisdictions using IT systems to support UOCAVA voting. For more detailed standards and guidelines, readers should consult the original NIST publications on a particular subject matter.

IT systems may be used to support UOCAVA voting in a variety of ways including managing or obtaining voter registration material, tracking requests for absentee ballots, providing or delivering blank ballots, or deploying remote electronic absentee voting systems. How information systems are specifically used to support UOCAVA voting will vary across jurisdictions, as different state and local jurisdictions have different procedures and systems for dealing with overseas voters. The appropriate security controls for these systems will be highly dependent on the type of systems that are deployed and how they are used. Since there are many potential ways to use IT systems to support UOCAVA voting, it is infeasible to provide detailed best practices for every possible architecture application, and configuration. Instead, this document provides a set of minimum security controls that should be applicable to any type of IT system used to support UOCAVA voting, including best practices for technical, physical personnel and procedural security of such systems.

The best practices in this document are intended to be broadly applicable to all voting systems supporting UOCAVA that leverage IT systems, but they do not cover all requirements for all UOCAVA voting systems. The baseline best practices provided must be augmented with additional safeguards depending on a jurisdiction's particular circumstances. After implementing the best practices described in this document, jurisdictions should carefully consider the type of UOCAVA voting system deployed, and its context of use to determine what additional security measures are required. It may not be possible to protect system-specific threats, such as those that would be unique to ballot delivery or return systems, using only the best practices described in this document. As described in NISTIR 7551 *A Threat Analysis on UOCAVA Voting Systems*, some types of UOCAVA voting systems face threats that are very difficult to mitigate with current technology, such as remote voting from personal computers. Jurisdictions must consider the potential threats to a UOCAVA voting system, along with the totality of security controls and measures implemented in the system, when determining whether the system is within an acceptable level of risk.

1.2 Intended Audience

This document contains detailed discussions of technical, procedural and managerial controls for information systems used to support UOCAVA voting. This document is directed toward readers who have a high degree of technical literacy of computer and network components, as well as computer security technologies. The primary audience for this document is technical personnel charged with implementing, deploying or maintaining UOCAVA voting systems. This includes technical support staff at state or local jurisdictions, vendors of products aimed at supporting UOCAVA voting, and service providers that host UOCAVA voting systems. It is important for jurisdictions to direct the information found in this document to the appropriate department or organization. In some cases, the individuals charged with supporting information technology equipment may not realize the equipment is used to support UOCAVA voting. For instance, technical staff may provide support for all county information systems, including those used by election officials and administrators for UOCAVA voting.

This document refers to system designers, implementers, operators, auditors and administrators. These roles are defined relative to the IT system used to support UOCAVA voting. They may not directly correspond to job titles within the organization(s) assembling, procuring, deploying or maintaining these systems. For example, an individual who holds the title “System Administrator” in an organization’s IT department may be charged with designing and deploying a system that sends blank ballots via email.

In addition, contracting officers, IT support staff, and other technical staff charged with making technical recommendations to policymakers may find this document useful as informative background material. Contracting officers may be able to identify specific security functionality that should be present in UOCAVA voting systems when evaluating products. Technical staff making technical recommendations to policymakers can use the background material in this document when weighing the advantages and disadvantages of different technical solutions to security issues. In addition, this document can be a useful guide for ensuring a jurisdiction employs a minimum baseline of security controls to protect UOCAVA voting systems and associated data.

2 General Overview

This section identifies the components that may be used to support UOCAVA voting and lists the technical security, operational and assurance controls that apply to the secure deployment, management and operation of the system.

IT systems facilitating UOCAVA voting can be used to support the following activities:

- Information delivery.
- Voter registration.
- Electronic blank ballot delivery.
- Remote electronic voting from controlled environments.
- Remote electronic voting from personally-owned systems.

The remaining sections of the document describe the controls in detail and offers guidelines for how these controls can be used to design, deploy and operate an overseas voting system. Because the roles of administering an election are different than the roles of administering an IT system, individuals are identified by their role relative to the system being deployed. This may not be the same as their role within the organization deploying the system. For example, a system administration team in a jurisdiction's IT department may be tasked with selecting, assembling, deploying and managing components used in a web application where voters can download blank ballots. Even though members of this team might be considered system administrators within the organization, relative to the voting system they are both designers and administrators.

Different sections of this document will be of more or less interest to the reader based on their role relative to the deployed UOCAVA voting system. Section 3 is primarily intended for designers of systems used to support remote absentee voting. The specific guidance in sections 4, 5 and 6 are intended for system administrators and other technical staff who will be charged with deploying the systems. These sections additionally provide important background material of interest to system designers. Section 7 is intended for systems administrators and technical staff who will be charged with the secure operation of these systems. Section 7 provides guidance for designers and other personnel tasked with selecting components which will be integrated into the voting system, along with informative background material for system administrators.

2.1 Overseas Voting Systems Components

The following identifies information technology components that may be found in IT systems deployed in support of overseas and military voters and explains the security objectives they can achieve. These components could exist as separate devices or multiple components may be located on a single device. For example, a firewall could be a hardware appliance on the network, a software process operating on each computer system, or both.

The components of an Internet-connected IT system supporting UOCAVA voting can be quite different than those used in a more traditional polling place voting systems. Polling place systems are often closed systems, where the voting system components, and any supporting infrastructure, are used only for conducting elections. An IT system that supports UOCAVA voting, particularly one that is Internet-connected, will almost certainly be a more open system. These systems may reuse a jurisdiction's existing communications infrastructure that is also used for important functions other than voting and elections. However, the IT systems that are directly used by election officials and voters rely on that infrastructure for important security protections. As such, this document contains best practices for IT components that may not be traditionally viewed as a component of a voting system, such as a hardware firewall appliance, or an intrusion detection system.

In this document, the term *server* is used to describe a computer system that primarily stores and/or manages data for various users and applications, and/or executes voting applications. The term *workstation* is used to describe a computer system that is used by a single user or limited number of users to perform individual tasks on the system itself or to access the servers.

An IT system facilitating UOCAVA voting may contain some or all of the following components:

- **Election Administration Components**
    - **Voter Registration Database:** Contains applicable information for registered voters.
    - **Administrative Console:** Used by the system administrators to manage the voting system, such as updating system software and monitoring event logs.

- **Election Official Workstation:** Used by the election officials to perform election related functions, such as creating ballot definitions and corresponding with voters via email.

- **Communications Components**
  - **Web Server:** Used to provide a browser-based interface and workflow for the users of the voting system.
  - **E-Mail System:** Used to send and receive e-mails from the voters, such as inquiries from voters, and attachments of blank ballots, and voter registration forms.
  - **Fax System:** Used to send blank ballots to the voters and to receive filled out ballots from the voters.
- **Security Components**
  - **Firewall:** Used to protect internal systems and network from unauthorized access and unauthorized communication traffic, and to block attack attempts from external systems and users.
  - **Intrusion Detection System (IDS) and Intrusion Prevention System (IPS):** Used to prevent and detect attacks attempted against the system and network, and to notify administrators.
  - **Authentication System:** Used for voters, election officials, and administrators to identify and authenticate themselves in order to perform their authorized functions.
  - **Public Key Infrastructure (PKI) Certification Authority (CA):** Used to issue public key certificates to web servers and users for use in Transport Layer Security (TLS) and other forms of authentication.
  - **Event Logging System:** Used to capture security and voting-related events in logs for accountability and forensic purposes.

This document covers only computer systems under the control of their respective election jurisdictions, or other parties designated by jurisdiction with the responsibility of operating those systems. As such, the security of voters' personal computers is not addressed in this document. However, voters may use jurisdiction-administered systems to interact with the voting system, as would be the case with kiosk-based systems. In these instances, jurisdiction-administered kiosks should be protected using similar controls to those used on election official workstations.

Remote overseas voting systems require information to be exchanged between the different components. How the information is exchange between components can take different forms. Information can be exchange between components by a connected set of computer systems such as a local or wide area network (LAN/WAN) or the Internet. Alternatively, physically moving storage media such as a disk or thumb drive between components can be used to exchange information. However information is exchanged between components, it needs to take steps to secure the exchange.

Not every overseas voting system will contain all of these components. For example, a system that merely delivers information to the voting public need not be connected to a voter registration database. It may also not need an e-mail system or a fax system. In systems that don't make heavy use of public key infrastructure, designers may opt to obtain and import certificates and revocation data from an external certification authority service rather than operate one as part of the voting system. However, most of the best practices described in this document will be applicable to any internet-connected system that is important to the election process. The implementation of these practices will often involve configuring and deploying security components, such as firewalls and intrusion detection systems.

2.2 Technical Controls

Technical security controls need to be established in the following areas in order to achieve the jurisdiction's security objectives for their UOCAVA systems:

1. ***Identification and Authentication (I&A)*** controls are used to establish the identity of a user and convey that identity to the system and applications running on the system.
2. ***Access Control*** uses the result of the I&A mechanisms to make a determination, either at the system or application level, whether a user is authorized to access data or perform operations on that data within the system.
3. ***Personally Identifiable Information (PII) Protection*** controls deal specifically with identifying and restricting the exposure of data that could be used to identify individuals while enabling sufficient access to this information that the system can function as intended.
4. ***Confidentiality*** controls detail mechanisms that ensure that potentially sensitive information about indviduals and about the system are is protected both in transit and at rest.

5. ***Integrity*** controls ensure that information critical to the proper functionality of the system cannot be undetectably altered in transit or at rest.
6. ***Availability*** controls are intended both to prevent situations which would render the system inoperable at critical times and to enable swift restoration of important functionality if these situations should arise.
7. ***Cryptographic Security*** controls support I&A, confidentiality and integrity protection using FIPS-standardized cryptographic mechanisms.
8. ***Communication Systems*** controls focus on maintaining the security and availability of the channels used to transmit data between the voting system and external systems and users.

Section 3 describes each category of control in detail and outlines specific options that may be available in various systems to support these. Section 4 expands on specific network-level protections required to enforce these controls. Section 5 discusses host-level protections used to implement these controls.

2.3 Operational Controls

Operational controls need to be established in the following areas in order to achieve the jurisdiction's security objectives for their UOCAVA systems

1. ***Facility Controls*** address physical security requirements for the equipment and wiring used to support the system.
2. ***Media Storage Controls*** establish physical and logical mechanisms for restricting the distribution of and access to media that contain sensitive information.
3. ***Personnel Security Controls*** are used to establish roles, duties and qualifications for those individuals tasked with operating the system.
4. ***Event Log Processing*** procedures are aimed at ensuring that system logs both constitute a complete record of system activity and are reviewed frequently enough to offer assurance that the system is operating as intended.
5. ***Backup and Archive*** procedures are intended to ensure both that a system can be audited in the future and that data sufficient to implement the Disaster Recovery controls is maintained.
6. ***Configuration Management*** controls ensure that a system is deployed and maintained in accordance with its functional and security objectives over its entire lifecycle.
7. ***Disaster Recovery*** controls are intended to ensure that an appropriate plan is established to enable restoration of system functionality in the event of unanticipated catastrophic failures.
8. ***Ongoing Testing*** is used to establish confidence that a system continues to meet its design goals.
9. ***Incident Handling*** processes establish a mechanism for reporting and remediation of security failures.
10. ***Removal from Service*** controls ensure both that the ability to audit events is preserved when systems are removed from service and that sensitive information is not exposed by systems that are no longer in service.

Section 6 describes these operational controls in detail and discusses their application to UOCAVA systems.

2.4 Assurance Controls

Assurance controls are subtly different from security controls. Where security controls are used to protect the data and functionality of a system in accordance with its design objectives, assurance controls serve two related purposes. First, they offer evidence that the security controls are in fact sufficient to meet these objectives. Secondly, they are used to establish confidence that these security controls are deployed and maintained. The assurance controls which are most important to UOCAVA systems fall into the following categories:

1. ***Documentation Requirements*** address both the design documents required to assure implementers that a given design meets the system's security objectives as well as documentation of those procedures necessary to install, configure and maintain the system in accordance with its design goals.
2. ***Vulnerability Analysis*** documentation offers evidence that potential vulnerabilities were considered and addressed during the design and deployment of a system.
3. ***Testing Requirements*** detail the test documentation used to establish that the above areas have been properly evaluated.

In short, assurance controls govern the documentation and testing required to demonstrate that the security best practices found in this document are followed for a particular system. The assurance controls take the form of design documentation to demonstrate how the system was designed to meet the IT security best practices, a vulnerability analysis explaining how common exploits for such systems and well-known security holes in system components are mitigated, and administrative guidance that instructs administrators in the secure operation of the system. Testing includes functional and penetration testing of the system performed as part of the development process. Assurance controls are described in detail in Section 7.

3 Security Controls

3.1 Identification and Authentication (I&A)

Authentication is the process of establishing confidence in the claimed identity of a user or system. Establishing the identity of a user is critical to the security of the system since the authenticated identity forms the basis for what actions the user can perform on the system and what information the user may access. Any IT system used to support UOCAVA voting will likely have several classes of users, each with their own set of rights and privileges on the system. The strength of authentication necessary depends on the consequences of an authentication error. As such, users with more privileged levels of access should, in general, be authenticated with a higher level of assurance. For example, three likely classes of users on an IT system supporting UOCAVA voting are system administrator, election officials, and voters.

This section summarizes guidelines from NIST Special Publication (SP) 800-63, *Electronic Authentication Guideline*, [SP800-63] and explains how these apply to UOCAVA systems in general. The primary audience for this section is system designers. Other readers should refer to this section and to [SP800-63] as needed.

In this section, we first offer general background information on the identification and authentication systems and then provide the best practices that are applicable and feasible for the various types of information technology systems described in Section 2.1. The remainder of this section is divided into the following subsections:

1. Threats to Credential Issuance Methods and Mitigations
2. Credential Issuance Methods
3. Threats to Authentication Mechanisms and Mitigations
4. Threats to Authentication Protocols and Mitigations
5. Types of Authentication Mechanisms
6. Best Practices for voting systems

3.1.1 Threats to Credential Issuance Methods and Mitigations

The issuance process is used by the users to establish trusted relationships with the authentication system and to obtain their authentication tokens[1]. The following subsections are examples of issuance mechanisms. Any gathered registration information (e.g., driver's license number, passport number, financial account information) should be protected as Personally Identifiable Information (PII) while in transit and while stored in the systems. The decision to store or delete this PII needs to be made based on the need to balance the protection of PII and the requirement to provide a basis for the legitimacy of voter registration records. For a more detailed discussion of PII protection, see section 3.3.

The following table provides a summary of threats to the credential issuance process and approaches to mitigate those threats.

Table 1: Threats to Credential Issuance Mechanisms and Mitigations

Threat/Attack	Threat Mitigation Mechanisms
Impersonation of claimed identity	In-person identity proofing by trusted party and the user providing Government issued photo IDs such as driver's licenses and passports to prove his identity. Additional assurance can be achieved by the user supplying a current document (e.g., last month's gas bill) with their name and address on it.
Repudiation of issuance	Have the individual sign a form acknowledging issuance of the token.

[1] The term *issuance* in this document includes some elements, such as verification of an applicant's identity, which are often referred to as *registration*. However, to avoid confusion between the voter registration process and the registration process for issuing credentials, only the term *issuance* is used in this document.

Threat/Attack	Threat Mitigation Mechanisms
Disclosure of Token	Issue token in person, or by physically mailing it in a sealed envelope to a secure location, or through the use of a communication protocol that protects the confidentiality of the session data.
Physical Theft of Token	Issue token in person or by physically mailing it in a sealed envelope to a secure location or via continuously tracked mail (e.g., registered mail, Federal Express, etc.)
Voluntary Disclosure of Token	A user may disclose their token in order to sell their vote. There is little protection against this threat.
Tampering of Token	Issue credentials in person, by physically mailing storage media in a sealed envelope, or through the use of a communication protocol that protects the integrity of the session data. Establish a procedure that allows the user to authenticate the source of token (e.g., digital signature on electronic transmission)
Unauthorized issuance	Establish procedures to ensure that the individual who receives the token is the same individual who participated in the registration procedure. For example, issue token in person, or physically mail it in a sealed envelope to the address of record of the user.

3.1.2 Credential Issuance Methods

Jurisdictions may establish a trusted relationship with a user and issue authentication tokens in-person, remotely, or using a combination of methods. For example:

a) ***In-person Issuance-*** Under this approach, the user appears before a trusted party. The trusted party authenticates the user on the basis of antecedent relationship or photo identification cards (e.g., drivers' license, passport). The user is issued a credential on the basis of this identity proofing in-person, online, or out of band.

b) ***On-line Issuance-*** Under this approach, the user accesses the authentication system online and provides information unique to the user that is not widely-known (e.g., bank account number, credit card number, account balances, passport number, etc.) The authentication system validates the information from authoritative databases and issues a credential online.

c) ***Out-of-Band Issuance-*** Under this approach, the user accesses the authentication system online and provides information unique to the user that is not widely-known (e.g., bank account number, credit card number, account balances, passport number, etc.) The authentication system validates the information from authoritative databases and issues a credential to the user to their address of record.

For voters, authentication credentials can be issued in association with voter identification or some other individually unique data set. Or jurisdictions could rely on credentials issued by some other trusted authority, such as the Department of Defense Common Access Card.

3.1.3 Threats to Authentication Mechanisms and Mitigations

Once credentials have been issued, authentication mechanisms allow users to provide another party with some level of assurance that they are who they claim to be. The follow table identifies high-level threats to authentication mechanisms and strategies for mitigating these threats.

Table 2: Threats to Authentication Mechanisms and Mitigations

Token Threat/Attack	Threat Mitigation Mechanisms
Theft	Use a password, PIN or biometric authentication to the token itself. The token locks up after a number of consecutive failed activation attempts.
Duplication	Use tokens that are difficult to duplicate, such as hardware cryptographic tokens.

Token Threat/Attack	Threat Mitigation Mechanisms
Discovery	Use authentication protocols in which the token cannot be discovered. Examples include supplying the token information over a Transport Layer Security (TLS) tunnel or using protocols such as Secure Shell (SSH) or Simple Authentication and Security Layer (SASL) with approved cryptographic algorithms.
Eavesdropping	Use authentication protocols in which the token cannot be captured by eavesdroppers. Examples include supplying the token information over TLS or using SSH and SASL-type protocols with approved cryptographic algorithms. Use tokens with dynamic authenticators where knowledge of one authenticator does not assist in deriving a subsequent authenticator. OTP and cryptographic protocols (e.g., client authenticated TLS) are examples of this.
Offline cracking	Use a token with a high entropy token secret. Long, randomly generated passwords and cryptographic keys with a security strength of 112 bits or higher are good examples.
Phishing or pharming	Use tokens with dynamic authenticators where knowledge of one authenticator does not assist in deriving a subsequent authenticator. OTP and cryptographic tokens are good examples. Use tokens that generate authenticators based on randomly generated input or challenge from authentication system. Cryptographic protocols such as TLS, SSH, and SASL, when used with approved cryptographic algorithms, are good examples.
Social engineering	Use tokens with dynamic authenticators where knowledge of one authenticator does not assist in deriving a subsequent authenticator. OTP and cryptographic tokens, when used with approved cryptographic algorithms, are good examples. Use tokens that generate authenticators based on randomly generated input or challenge from authentication system. Cryptographic protocols such as TLS and SSH are good examples.
Online guessing	Use a token with a high entropy token secret. Long, randomly generated passwords and cryptographic keys with a security strength of 112 bits or higher are good examples. Use a token that locks after a number of repeated failed activation attempts.

3.1.4 Threats to Authentication Protocols and Mitigations

Some of the threats such as eavesdropping, phishing, pharming, and online guessing have been discussed above. The following table provides additional threats that arise for authentication protocols and how to mitigate those threats.

Table 3: Threats to Authentication Protocols and Mitigations

Authentication Protocol Threat/Attack	Threat Mitigation Mechanisms
Replay	Cryptographic protocols that use nonces, sequence numbers, or challenges. TLS is an example of such a protocol.
Session Hijacking	Cryptographic key derived from the authentication process is used to authenticate all session data (e.g., individual packets). TLS is an example of such a protocol. Note: Application-level concerns arising from session hijacking are mitigated by layering this authentication and following the practices outlined in section 5.10.

Authentication Protocol Threat/Attack	Threat Mitigation Mechanisms
Man-in-the-middle	Cryptographic protocols that protect the user from revealing information (e.g., authentication secret) to an attacker masquerading as the authentication system. Client authenticated TLS is an example of such a protocol; due to the mechanisms in the protocol, a masquerading party cannot make the user sign the appropriate secret to complete the man-in-the-middle attack. In the case of websites served over HTTPS, server side-only TLS is also protected from this threat so long as the user is not deceived into using an attacker's Uniform Resource Locator (URL). Commercial products will warn users of this deception so long as no certification authority trusted by the user acts improperly by issuing a certificate to an attacker attempting to pose as the legitimate authentication system.

3.1.5 Types of Authentication Mechanisms

Authentication mechanisms are broken down in two broad categories: token based and biometric. Material developed in this section is based on [SP800-63]. That document, particularly Sections 7 and 8, may be consulted for additional background and technical information.

3.1.5.1 Token Based Authentication

Token based authentication relies on the user demonstrating possession and control of something that can be used to establish identity. This can incorporate one or more of three factors: something the user has, something the user knows, or something the user is. The system uses an authentication protocol to validate the user's possession and control of the token. There are various types of tokens that may be used depending on the capabilities and assurance requirements of the system authenticating the user. These are described in detail below.

a) ***Memorized Secret Tokens-*** Using memorized secret tokens, users prove their identities by providing a secret known to them and verifiable by the authentication system. Passwords and Personal Identification Numbers (PINs) are good examples of memorized secret tokens. This secret needs to be established during the user registration process. User Identifier (ID) and password for a computer account, or a PIN for unlocking a cryptographic token are examples of memorized secret tokens. The advantages of the memorized secret tokens are ease of use and wide availability in commercial products. Disadvantages of this approach and their corresponding mitigations, where possible, are listed below:

   i) The token can be revealed to unauthorized parties during token issuance. This threat can be mitigated by issuing the token using a protected channel such as in-person hand-off or sending the token to an address of record via continuously tracked mail; or protecting the electronic communication channel used for token issuance.

   ii) The token can be revealed via "shoulder surfing" while being presented (entered or typed in) for authentication. This threat can be mitigated by not echoing the token when it is entered.

   iii) The token is written down and hence can be accessed by unauthorized parties. This threat can be mitigated by memorizing the token or by protecting the written down value.

   iv) The token can be obtained by eavesdropping during the authentication process. This threat can be mitigated by cryptographically protecting the authentication channel or by using authentication protocols that prove the possession of the token without revealing it.

   v) An unauthorized party can use manual or automated means to authenticate by providing values for the token until authentication succeeds (e.g., performing an online dictionary attack). This threat can be mitigated by locking the account after a small number of unsuccessful authentication attempts, or by introducing a delay between unsuccessful authentication attempts that increases after each failure.

   vi) An attacker can mount an offline dictionary attack by eavesdropping on the protected protocol. This threat can be mitigated by avoiding protocols that are susceptible to offline dictionary attacks. Users are generally incapable of generating or remembering passwords that are strong enough to prevent an offline dictionary

attack (17 randomly chosen characters,) and may compromise the security of passwords by writing them down.

vii) The legitimate token owner can provide the token to someone else in a vote buying scheme or can be tricked into sending the password to a party impersonating the legitimate voting system. There is no easy mitigation to this threat.

viii) Malware on a user's computer can capture the token as it is entered by the user, and pass it on to an unauthorized party. Up-to-date and activated antimalware software can mitigate this threat on administered systems.

b) Pre-registered Knowledge Token- Under this authentication approach, a user establishes a set of questions and answers during the user registration process with the authentication system. In order to be effective, questions and answers should be easy for the user to recall from memory, and difficult for others to obtain or guess. Authentication is based on the accuracy of the responses provided by the user. An example of a Pre-registered Knowledge Token would be a question such as "What was the first car you ever owned?" and requiring the answer to contain the year, make, model and color. Based on the accuracy of the responses supplied by the user, the authentication system determines if the attempt is successful or not. Another example is asking the user to select an image or set of images that the user memorizes during the registration phase; the user then has to identify the correct images from a set(s) of similar images. Note that pre-registration is different from Knowledge Based Authentication (KBA); in KBA the answers are verified by querying a database containing information about the user. The advantages of the pre-registered knowledge tokens are ease of recall, ease of use and wide availability of commercial implementations. Disadvantages of this approach and their corresponding mitigations, where possible, are listed below:

i) The token can be revealed to unauthorized parties during token registration. This threat can be mitigated by using a protected communication channel during the token registration.

ii) The token can be revealed via "shoulder surfing" while being registered or presented (entered or typed in) for authentication. This threat can be mitigated by not echoing the knowledge as it is input. In such a case, during input, the knowledge may need to be entered twice to protect against typing errors.

iii) The token can be obtained by eavesdropping during the authentication process. This threat can be mitigated by cryptographically protecting the authentication channel or by using authentication protocols that prove the knowledge of the token without revealing it.

iv) An unauthorized party can use manual or automated means to authenticate by providing values for the token until authentication succeeds (e.g., performing an online dictionary attack). This threat can be mitigated by locking the account after a small number of unsuccessful authentication attempts, or by introducing a delay between unsuccessful authentication attempts that increases after each failure.

v) An attacker can mount an offline dictionary attack by eavesdropping on the protected protocol. This threat can be mitigated by avoiding protocols that are susceptible to offline dictionary attacks.

vi) The knowledge which is prompted for could be discoverable by searching public records or social networking sites. Mitigation of this threat is difficult. That is why this mechanism is generally used as an added secondary authentication mechanism.

vii) The legitimate token owner can provide the token to someone else in a vote buying scheme, or can be tricked into sending the token to a party impersonating the legitimate voting system. There is no easy mitigation to this threat

viii) Malware on a user's computer can capture the token as it is entered by the user, and pass it on to an unauthorized party. Up-to-date and activated antimalware software can mitigate this threat on administered systems.

c) Look-Up Secret Token- Under this authentication approach, the user and the authentication system share one or more secrets that are held in a physical or electronic medium by the user. The user uses the token to look up the appropriate secret(s) that are needed to respond during authentication. For example, a user may be asked by the authentication system to provide a specific subset of the numeric or character strings printed on a card in table format. If the user is able to provide the correct response, the user is successfully authenticated. The shared secret(s) needs to be established during the user registration process. The advantages of look-up secret tokens are

that they are less susceptible to eavesdropping and to online and offline dictionary attacks. Disadvantages of this approach and their corresponding mitigations, where possible, are listed below:

i) The implementation of these tokens requires additional software and possibly hardware on the authentication server side, resulting in increased cost.

ii) If the token is hardware based, this further increases the overall cost.

iii) The tokens are not as easy to use as a static secret token.

iv) The tokens cannot be memorized and hence must be stored in hardware, software, or printed form.

v) The token can become unusable due to malfunction or availability. For example, hardware tokens can stop functioning, software list of secrets can get corrupted or become otherwise un-accessible, tokens can be misplaced or can become unreadable (e.g., due to fading or smudging).

vi) The token can be revealed to unauthorized parties during token issuance. This threat can be mitigated by issuing the token using a protected channel such as in-person hand-off, or sending the token to address of record via continuously tracked mail; or cryptographically protecting the electronic communication channel used for token issuance.

vii) The token can be obtained by eavesdropping during the authentication process, if the token secret space is limited (e.g., grids). This threat can be mitigated by cryptographically protecting the authentication channel.

viii) An unauthorized party can use manual or automated means to authenticate by providing values for the token until authentication succeeds (e.g., perform an online dictionary attack). This threat can be mitigated by locking the account after a small number of unsuccessful authentication attempts.

ix) The legitimate token owner can provide the token to someone else in a vote buying scheme, or can be tricked into sending the token to a party impersonating the legitimate voting system. There is no easy mitigation to this threat.

x) Malware on a user's computer can capture the token as it is entered by the user, and pass it on to an unauthorized party. Up-to-date and activated antimalware software can mitigate this threat on administered systems.

d) Out of Band Token- Under this authentication approach, a secret authenticator is transmitted from the authentication system to a physical device or system controlled by user. The communication channel for this transmission must be separate from the communication channel used for user authentication. The secret authenticator transmitted is valid for one time use and expires within minutes. An example of out of band token is as follows: a user attempts to log into a website and receives a password or PIN on his or her cellular phone, PDA, pager, or land line which the user must enter in the web session in order to be authenticated. Note that the user cellular phone, PDA, pager, or land line number is registered during the user registration process. The advantages of the out of band tokens are that they mitigate the threat of eavesdropping (attacker is less likely to succeed in eavesdropping two channels, particularly with the second one existing only for a very short duration), and thus, also protecting against successful online or offline dictionary attacks against the authentication secret. The disadvantages of this approach and their corresponding mitigations, where possible, are listed below:

i) The destination of the token (e.g., specific phone number) could be specified by the attacker during issuance. This threat can be mitigated by using a protected channel for token channel registration such as in-person hand-off or cryptographically protecting the electronic communication channel used for token channel registration.

ii) Most commercial products require enhancement or additional commercial products to implement the out of band tokens, resulting in higher costs.

iii) The user being authenticated requires the second channel. Not all voters may have access to a second.

iv) The legitimate token owner can provide the token to someone else in a vote buying scheme, or can be tricked into sending the token to a party impersonating the legitimate voting system. There is no easy mitigation to this threat, but using the second channel requires the voter to register another party's channel (resulting in possible detection during auditing) or to be present to cast a ballot.

v) Malware on a user's computer can capture the token as it is entered by the user, and pass it on to an unauthorized party. The one-time nature of these tokens requires a more sophisticated attack whereby the

malware must pass the captured token for immediate use by an attacker.

e) One Time Password (OTP) Device- this authentication approach, the user holds a hardware device that supports the spontaneous generation of one time passwords. The authentication system is synchronized with the hardware device. Authentication is accomplished by providing an acceptable one time password from the device. These devices themselves may or may not require biometric or password/PIN authentication in order to generate the one time password. The synchronization of the hardware device with the authentication system needs to be established during the user registration process. The advantages of OTP tokens are that they are not susceptible to online or offline dictionary attacks, and are not susceptible to eavesdropping. Disadvantages of this approach and their corresponding mitigations, where possible, are listed below:

i) The implementation of these tokens requires additional software and possibly hardware on the authentication server side, resulting in increased cost.

ii) The token is generally hardware based, adding to the cost.

iii) The token can be provided to unauthorized parties during token issuance. This threat can be mitigated by issuing the token using a protected channel, such as in-person hand-off or sending the token to address of record via continuously tracked mail.

iv) The token can be stolen. This can be mitigated by user vigilance, by adding a secret PIN or password to the OTP, and/or by using the device with a biometric. The biometric, secret PIN or password could be used in a variety of ways depending on the OTP implementation. It could be used to unlock the token, could be input to create the OTP, or could be simply appended to the OTP.

v) The token can become unusable due to malfunction.

vi) The token may be deemed difficult to use. If the token and the authentication server are out of synchronization, the protocol may automatically synchronize or may require the user to perform additional actions until the token is brought back in synchronization with the authentication server.

vii) The legitimate token owner can provide the token to someone else in a vote buying scheme, or can be tricked into sending the token to a party impersonating the legitimate voting system. There is no easy mitigation to this threat.

viii) Malware on a user's computer can capture the token as it is entered by the user, and pass it on to an unauthorized party. The one-time nature of these tokens requires a more sophisticated attack whereby the malware must pass the captured token for immediate use by an attacker.

f) Cryptographic Token- Under this authentication approach, a cryptographic key token is held by the user. The token could be hardware based (e.g., a smart card or Universal Serial Bus (USB) form factor cryptographic module) or could be software based (e.g., CD or USB storage device). Furthermore, the token could perform functions with or without local authentication. Local authentication could be biometric or password/PIN based. Authentication is accomplished by proving possession of the cryptographic key by performing a cryptographic key based operation during an authentication protocol (e.g., challenge – response). For example, a public, private key token is held by the user and the user performs a digital signature on a random challenge from the authentication server. User authentication via client-authenticated TLS is an example of such protocol. The association of cryptographic key with the user needs to be established during the user registration process or using other means such as Public Key Infrastructure (PKI). The advantages of the cryptographic tokens are that they are not susceptible to online or offline dictionary attacks, and are not susceptible to eavesdropping. Disadvantages of this approach and their corresponding mitigations, where possible, are listed below:

i) The implementation of these tokens requires additional software on the authentication server side, but this is not a significant disadvantage since the software is part of commercial products and comes bundled in resulting in no added cost except for requiring some additional time to configure the system.

ii) If the token is hardware based, it adds to the cost.

iii) The token can be provided to unauthorized parties during token issuance. This threat can be mitigated by issuing the token using a protected channel such as in-person hand-off, sending the token to address of record via continuously track mail, or providing the token in a protected communication channel.

iv) The token can be stolen. This can be mitigated by user vigilance, by adding a secret PIN to the token, and/or by using the token with a biometric. The secret PIN or biometric can be used to unlock and use the token.

v) The token can become unusable due to malfunction.

vi) The legitimate token owner can provide the token to someone else in a vote buying scheme. There is no easy mitigation to this threat.

vii) Malware on a user's computer can capture the cryptographic token, and any tokens entered by the user to unlock the cryptographic token, and pass it on to an unauthorized party. Hardware-based cryptographic tokens can significantly mitigate this threat.

3.1.5.2 Biometric Authentication

Under the biometric authentication approach, the user is authenticated based on one or more intrinsic biological traits such as fingerprint, iris, face, voice, palm, or other characteristics that cannot be forged. Such systems do not provide perfect authentication since there are always false positives in which another person's biometric information is deemed to match that of the user, or false negatives in which a legitimate user's information is rejected due to an error in scanning the biometric data. In addition, physical handicaps can prevent an individual from using a biometric authentication mechanism, for example, an amputee may not have fingerprints. Biometric mechanisms are also vulnerable to capture and replay attacks unless compensating means such as cryptographic and "liveness" properties (such as a nonce or a challenge) are included to mitigate the capture and replay threat. These mechanisms are generally used only as a second factor (e.g., to unlock one-time password devices or cryptographic tokens). Furthermore, these mechanisms are generally used locally or to locally authenticate someone in the presence of a trusted individual (e.g., fingerprint scan in the presence of a guard while entering or exiting a secure facility)).

3.1.6 Best Practices for Voting Systems

The authentication mechanisms discussed above offer differing levels of assurance about the user's identity and carry differing associated costs. Furthermore, not all authentication mechanisms are feasible for all products. The security criticality of the various functions should be weighed against the cost inherent in and assurance provided by the available I&A options. [OMB0404] offers guidelines for considering the potential impact of authentication failures and the likelihood of that impact should a failure occur. Section 2.2 of [OMB0404] provides guidance on making the identified risks to the appropriate authentication assurance level. [SP800-63] offers technical guidance for mapping authentication mechanisms to the results of this assessment.

In assessing the risks associated with authentication failure in a UOCAVA system, it is helpful to consider three broad classes of users: administrative personnel, election officials and voters.

Administrative personnel require access to the system in order to install, configure and operate the software. These personnel are critical to the security of the system; should an unauthorized entity gain administrative control of the system, the integrity of the UOCAVA voting system could be compromised. This constitutes high harm to agency programs and public interests. One or more compromised administrative accounts could also lead to release of personal voter information to unauthorized parties on a large scale. As a result, administrative personnel should be authenticated in accordance with assurance level 4 in order to perform their duties, as [OMB0404] describes assurance level 4 as being "*appropriate for transactions needing very high confidence in the asserted identity's accuracy.*" Thus, in accordance with the guidance published in [SP800-63], in-person identity proofing should be required to register administrative personnel and a hardware cryptographic token over a secure channel should be used for authentication.

Election officials require access to the system in order to configure the voting application, conduct the election, and audit the results. These personnel are likewise critical to the security of the system; should an unauthorized entity improperly access the system and assume the role of an election official, integrity of the UOCAVA voting system could be compromised. This constitutes high harm to agency programs and public interests. As a result, election officials should also be authenticated in accordance with assurance level 4 in order to perform their duties. The same level of identity proofing and authentication control should apply to election officials as to administrative personnel.

Voters require much more limited access to the UOCAVA system. In a properly controlled system, compromise of a single voter account would lead to, at most, the compromise of a single vote. The limited impact of a compromised identity in this case suggests that authenticating voters should require at least assurance level 2 as described in [OMB0404]: "*Level 2 credentials are appropriate for a wide range of business with the public where agencies require an initial identity assertion (the details of which are verified independently prior to any Federal action).*" According to [SP800-63], level 2 credentials include a password sent over a secure channel. However, a higher assurance level would be needed to mitigate phishing, man-in-the-middle, and certain malware attacks.

In all three cases, the secure channel employed should be TLS with a cipher suite that provides 112-bit security or greater and where the X.509 certificates are validated according to the algorithm in [RFC5280]. TLS should perform mutual authentication for administrative access, and perform at least server-side authentication for voters connecting to the system.

3.2 Access Control

Access control technology deals with providing access to the stored information such as files, directories and functions to authorized users and denying that access to others. I&A and Access Control go hand in hand. I&A is performed in order to gain assurance of the user's identity. Once the identity of the user is established, an access control decision based on this authenticated identity appropriately enforces the system access control policy. Thus, first performing I&A, and then performing access control based on authenticated identity are required to enforce the security of an Information Technology (IT) system. The primary audience for this section is voting system designers.

Access control mitigates the threat of unauthorized actions such as access to or modification of the data or attempting to perform unauthorized functions. If administrative actions are not properly controlled, the security controls of the entire voting system can be defeated by the person who can bypass administrative access controls. The compromise may include the unauthorized person determining the outcome of the election. If voter actions are not properly controlled, any of the following can be compromised: voter personally identifiable information, voter election choices, and unauthorized vote casting.

Protection of information in transit is dealt with using technologies such as cryptography and protected communication links and is discussed elsewhere in this document.

The remainder of this section is divided into the following subsections:

1. Types of Access Control Mechanisms
2. Threats to Access Control Mechanisms
3. Best Practices for Voting Systems

3.2.1 Types of Access Control

The following are examples of access control mechanisms:

1. Discretionary Access Control (DAC)
2. Role Based Access Control (RBAC)
3. Privilege/Attribute Based Access Control (PBAC/ABAC)
4. Mandatory Access Control (MAC)
5. Type Enforcement
6. Capability Based Access Control (CBAC)

3.2.1.1 Discretionary Access Control (DAC)

DAC is the mechanism where the owner or the creator of the information determines who can have what type of access to the information.

The type of access is also termed "access mode" and refers to the types of operations that can be performed on the information or the object containing the information. Examples of types of operations that may be protected with DAC include: read, write, execute (for program files), search (for directories/folders), list (for directories/folders), etc.

DAC is widely implemented in today's commercially available operating systems such as Unix, Linux, and Windows.

Unix protection bits are an example of DAC. Each file or directory has 3 sets of bits, each set containing 3 bits for a total of nine bits. One set of bits represents permissions for the individual owner of the object (read, write, or execute[2]). The

[2] Read permission for a directory is interpreted as the ability to list the contents of a directory. Write permission to a directory is interpreted as ability to create files and subdirectories underneath the directory. Execute permission for directory is interpreted as the ability to search the directory.

second set of bits represents permissions for the owning group of the object[3]. The third and final set of bits represents permissions for all other users and groups.

Another example of DAC in wide use in operating systems is Access Control List (ACL). Conceptually an ACL is a collection of Access Control Entries (ACEs). Each ACE contains a user, group, or role name and access mode. In some implementations even delegation is supported by either including access modes for delegation in ACE or by having special ACE entries for delegation.

Fine-grained DAC is supported using similar concepts at application level data in many commercial products. For example, Relational Data Base Management System (RDBMS) can support ACL for rows, columns, tables, views, stored procedures, etc.

3.2.1.2 Role Based Access Control (RBAC)

RBAC is similar to DAC except that an individual's role dictates what information or functions that individual can access. The RBAC is defined by roles and the permitted operations for a role on a given object. Thus, conceptually, RBAC can be viewed as (and can be implemented using) ACL and ACE, where subject of the entries is a role rather than named users or groups. For example, in a system that implements RBAC, only users assigned the role of "auditor" might be permitted to read audit log entries, and only users assigned the role of "registration authority" would be permitted to create new users.

RBAC can be made hierarchical by adding relations for supporting role hierarchies where a role has all the authorizations of all the subordinate roles.

RBAC is implemented using DAC in commercial operating systems and in RDBMS.

RBAC can be viewed as a DAC mechanism if the object owner determines to share the object based on role.

RBAC can be viewed as MAC if the system makes the determination to share the object based on role instead of the object's owner/creator.

3.2.1.3 Privilege/Attribute Based Access Control (PBAC/ABAC)

PBAC is akin to RBAC except that privileges are atomic rights. A role can be viewed as collection of privileges. Access control for data and functions is implemented using PBAC in commercial operating systems and in RDBMS.

3.2.1.4 Mandatory Access Control (MAC)

MAC is also called label-based access control. It is termed mandatory because the inputs for the access control policy are system determined and are not at the discretion of the object's owner/creator. Objects and user sessions are assigned security labels by the system, and access decisions are enforced based on the compatibility of these labels. Not many commercial products offer MAC. For a more detailed explanation of MAC, see [TCSEC].

3.2.1.5 Type Enforcement

Type enforcement is another form of mandatory policy. The policy is enforced based on "domain definition" table. A "domain definition" table consists of rows representing domains of execution and types representing object type and cells consisting of "access mode". In order for a process to perform an operation on an object, the cell representing the execution domain of the process and object type is examined to determine if the "access mode" representing the operation is permitted.

There are not many commercial products offering type enforcement.

3.2.1.6 Capability Based Access Control (CBAC)

CBAC consists of the object owner obtaining the object capability (e.g., a handle or random number) when the object is created. The object owner can pass this capability to others. Thus having the object access information is an implicit right to access the object.

There are not many commercial products offering CBAC.

[3] Owning group is defined as the group the user session was invoked with when the object was created.

3.2.2 Threats to Access Control Mechanisms

The following table provides a summary of threats to the access control mechanisms and approaches to mitigate those threats.

Table 4: Threats to Access Control Mechanisms

Threat/Attack	Threat Mitigation Mechanisms
Access control modified by the user	Access control is implemented in a protected operating system
Access control bypassed by the user	All object access is mediated by the operating system so that the operating system can enforce the access control policy
Fine-grained application-based access exploited by the user to gain greater access	Application control fine-grained objects implemented using operating system object. These objects are under the control of the operating system and owning application only.
One application accessing another application's objects	Application control fine-grained objects implemented using operating system object. These objects are under the control of the operating system and owning application only.
Resource exhaustion covert channels against MAC	Use trusted application so that the channels cannot be exploited Audit the channels Eliminate the channel by sound design and by reducing resource sharing
Other storage channel attacks against MAC	Use trusted application so that the channels cannot be exploited Audit the channels Eliminate the channel by sound design and by reducing resource sharing
Timing channel attacks against MAC	Use trusted application so that the channels cannot be exploited Audit the channels Eliminate or reduce the channel capacity by using fixed time slices where possible.

3.2.3 Best Practices for Voting Systems

In general, the voting system designer should use an operating system and commercial applications that provide DAC. The voting system application should implement RBAC using these DAC facilities. Functions associated with the configuration, use and maintenance of the voting system application should be assigned to named roles, and these roles should be assigned to users or groups of users. Users should only be permitted to perform the functions associated with their roles when the role is active and the user has authenticated. So, for example, the role associated with the "register new voters" function might only be activated at certain times. The system should ensure that the role is both assigned to the user and active for the authenticated session.

3.3 Personally Identifiable Information (PII) Protection

The Government Accountability Office defines personally identifiable information (PII) as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[GAO08536] Election authorities should consult relevant state and local laws to determine if there are governing definitions for PII in their jurisdiction.

Examples of PII include, but are not limited to:

- Name, such as full name, maiden name, or mother's maiden name.
- Personal identification number, such as social security number (SSN), passport number, driver's license number, or financial account number.

- Contact information, such as street address or email address.
- Personal characteristics, including photographic image, handwritten signatures, or biometric data.

Not all PII must be protected equally. Section 3 of NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information,* identifies six factors that organization should consider when determining the appropriate level of protection. Organizations should consider the following:

- How easily the PII can be tied to specific individuals.
- The number of individuals whose PII is stored in the system.
- The sensitivity of the data.
- The context of how the data will be used, stored, collected, or disclosed.
- Legal obligations to protect the data
- The location of the data, and level of authorized access to the data.

Further guidance on what constitutes PII, factors that influence PII sensitivity, and how PII should be handled from collection to destruction is provided in NIST SP 800-122, *A Guide to Protecting the Confidentiality of Personally Identifiable Information* [SP800-122]. The guidance in this section primarily applies to voting system designers and technical staff charged with protecting sensitive information on voting system equipment. The best practices outlined in this section should be used by election officials as a baseline for determining the appropriate controls to protect any PII stored by the jurisdiction. Based on the factors identified above, an organization may decide that additional protection is needed, or that some of the practices can be relaxed.

For the purpose of a voting system, PII identified in Section 3.3.1 is considered linked and highly sensitive. The rest of the guidance is formed on that basis.

The following subsections discuss the protection of PII:

1. Information Identified as PII
2. Threats to PII
3. Mechanisms for PII Protection while in Transit
4. Mechanisms for PII Protection while in Storage

For additional discussion of safeguards to protect the confidentiality of PII, see Sections 4 and 5 of [SP800-122].

3.3.1 Personally Identifiable Information (PII)

The following are examples of PII that may be found in a voting system:

1. Information in the voter registration database:
    a) Voter Name
    b) Voter Address
    c) Voter Contact information (e.g., phone number(s), e-mail address, etc.)
    d) Voter Political affiliation
2. Information used to verify voter identity during voter registration. Examples include one or more of the following:
    a) Driver's License Number
    b) Passport Number
    c) Bank Account Number
    d) Credit Card Number

3.3.2 Threats to PII

The following table details threats to PII along with possible mitigation mechanisms.

Table 5: Theats to PII

Threat to PII	Threat Mitigation Mechanisms
Unauthorized disclosure during transit	Encrypt the PII with FIPS validated encryption algorithm using appropriate key size so that only the authorized recipient can successfully decrypt the PII. Physically carry the PII or send it via physically protected paper mail.
Unauthorized modification during transit	Cryptographically protect the PII using FIPS validated algorithm using appropriate key size so that the recipient can verify the integrity of PII. Examples of cryptographic integrity protection are digital signatures, HMAC, or Cipher-based Message Authentication Code (CMAC) Physically carry the PII or send it via physically protected paper mail.
PII can be obtained by an attacker who gains access to a computer system where it is stored	Use a mix of computer security controls, firewalls, and IDS/IPS to deny attackers access to information including PII. Only store the PII that is required to be maintained. Only store the PII for the duration it is required. PII in storage can be cryptographically protected using FIPS validated algorithm, using a key that is stored off the system, or that must be unlocked with something stored off the system.
PII can be modified by an attacker who gains access to a computer system where it is stored	Use a mix of computer security controls, firewalls, and IDS/IPS to deny attackers access to information including PII. Store PII on non-rewritable media (e.g., Write-Once Read Many (WORM))
PII can be obtained by an unauthorized user of a computer system where it is stored	Use a mix of computer security controls provided by a secure operating system that requires identification and authentication. Use the access control mechanisms of the secure operating system to provide access to the PII.
PII can be modified by an unauthorized user of a computer system where it is stored	Use a mix of computer security controls provided by a secure operating system that requires identification and authentication. Use the access control mechanisms of the secure operating system to provide access to the PII. Configure the access control on PII to prohibit modification. Store PII on non-rewritable media (e.g., WORM)
Stored PII can be inappropriately accessed (viewed) by authorized personnel	Use a mix of computer security controls provided by a secure operating system that requires identification and authentication, and provides access control mechanisms. Use the access control mechanisms to restrict PII access to administrators. Require multi-person control for access to administrative accounts using a combination of technical and procedural controls. Examine event logs regularly to determine if PII is being accessed for unauthorized purposes by authorized users. Encrypt the PII and provide access to the decryption key to someone other than the person having access to PII.

Threat to PII	Threat Mitigation Mechanisms
Stored PII can be inappropriately modified by authorized personnel	Use a mix of computer security controls provided by a secure operating system that requires identification and authentication, and provides access control mechanisms. Use the access control mechanisms to restrict PII modification to administrators. Require multi-person control for access to administrative accounts using a combination of technical and procedural controls. Store PII on non-rewritable media (e.g., WORM) in an encrypted format.

3.3.3 Best Practices for Protection of PII in Transit

The voter PII in transit electronically should be secured using FIPS 140-2 validated cryptography, using FIPS algorithms, 112 bit security, and standardized Internet protocols. Examples of such mechanisms include:

1. TLS that is based on 2048 bit Rivest, Shamir, Adelman (RSA) certificates, using 3 key Triple Data Encryption Standard (TDES) and SHA-1[4] or SHA-2.
2. Internet Protocol Security (IPSec) that is based on 3 key TDES or Advanced Encryption Standard (AES) encryption and based on a 2048 bit Diffie Hellman (DH) Group for key exchange and 2048 bit RSA for end point authentication.

3.3.4 Best Practices for Protection of PII in Storage

Personally identifiable information should be provided only to the authenticated voter and other authorized individuals.

Personally identifiable information should be protected from unauthorized access and disclosure while it is stored in the voting system. At a minimum, the native operating system access control enforcement mechanism should be used to protect the voter PII storage container (e.g., file or database). These protection mechanisms should permit only authorized voting system applications access to the voter database. Additional application level DAC should be implemented so that only authorized users whose identity has been properly authenticated can access the voter PII. An example is a database with a DBMS that offers fine grained DAC based on tables, rows, columns, and views. The user authentication can be obtained from the underlying operating system or the DBMS can perform its own authentication. The user role is derived from the authenticated identity.

Given the Commercial-Off-The-Shelf (COTS) capabilities, administrators are likely to have access to the PII discussed above. One method mitigating the threat of abuse by administrators is to enforce separation of administrative duties. This could be accomplished with multi-person physical control to the system and administrative functions while prohibiting remote access. Note that multi-person administrative control can also be achieved by strictly limiting remote access to a workstation that is under the same multi-person physical control and has the following additional security controls:

1. The remote workstation has the same computer security controls as the voting system
2. The remote workstation is connected to no other networks but the voting system and uses FIPS validated, 112 bit security FIPS algorithms, Internet approved protocols (e.g., TLS, IPSec, etc.) to secure the communication channel between the remote workstation and the voting system.
3. The communication protocol used provides for mutual authentication, integrity and confidentiality.

[4] SHA-1-based HMAC is considered to offer security commensurate with the key size as opposed to 80 bits.

3.4 Confidentiality

If the confidentiality of information is not protected, it can lead to the compromise of PII (leading to identity theft, blackmail, embarrassment, etc.) or to a masquerading party obtaining information that can be used to authenticate as an administrator, election official, or voter. The masquerading in turn can lead to threats listed in Section 3.1. The primary audience of this section is system designers.

Table 6: Threats to Confidentiality

Threat to Confidentiality	Threat Mitigation Mechanisms
Information can be obtained during transit	Encrypt the information with FIPS validated encryption algorithm using appropriate key size so that only the authorized recipient can successful decrypt PII. Physically carry the information or send it via physically protected paper mail.
Information can be obtained by an attacker from a computer system where it is stored	Use a mix of computer security controls, firewalls, and IDS/IPS to deny attackers access to information.
Information can be obtained by an unauthorized user of a computer system where it is stored	Use a mix of computer security controls provided by a secure operating system that requires identification and authentication. Use the access control mechanisms of the secure operating system to provide access to the information.
Stored Information can be inappropriately accessed (viewed) by authorized personnel	Use a mix of computer security controls provided by a secure operating system that requires identification and authentication, and provides access control mechanisms. Use the access control mechanisms of the secure operating system to restrict access to the information. Encrypt the information and restrict access to the decryption key to someone other than the person having access to the information, effectively providing two person control. Regularly review event log for access events and rely on event log monitoring as a deterrent.

The following subsections discuss the confidentiality of information:

1. Information Requiring Confidentiality Protection
2. Confidentiality Mechanisms for Information in Transit
3. Confidentiality Mechanisms for Information in Storage

3.4.1 Information Requiring Confidentiality Protection

Voter PII protection has been addressed in Section 3.3. This section addresses confidentiality of other voter information.

The following are examples of information that require confidentiality protection:

1. Cast ballots should not be accessible to system administrators.
2. Event logs (both the operating system and application) should be accessible only by the administrators.
3. Passwords and private and secret keys should be protected from unauthorized access or use.

3.4.2 Best Practices for Confidentiality Protection of Information in Transit

Information requiring confidentiality protection which is electronically transmitted should be secured using FIPS 140-2 validated cryptography, using FIPS algorithms, 112 bit security, and standardized Internet protocols. Examples of such mechanisms include:

1. TLS that is based on 2048 bit RSA certificates, using 3 key TDES and SHA-1 or SHA-2. In TLS, each packet is encrypted using TDES or AES algorithm using a secret key that is securely established during the TLS connection formation.
2. IPSec that is based on 3 key TDES or AES for encryption, 2048-bit DH Group for key exchange, and 2048 bit RSA for end-point authentication. Authentication is based on either TDES Cipher Block Chaining (CBC) mode, SHA-1 based HMAC, or AES Counter with CBC Message Authentication Code (CCM) mode. DH is used to negotiate shared session key. The shared session key in turn is used for TDES or AES encryption of data.

3.4.3 Best Practices for Confidentiality Protection of Information in Storage

Information requiring confidentiality protection should be provided only to the authorized individuals.

Information requiring confidentiality protection should be protected from unauthorized access while it is stored in the voting system.

When the ballot information is no longer required, it should be erased. Such information may require retention to support audit, and federal law requires the retention of election-related data for 22 months. It is recommended that upon the close of the election such information should be archived, with archival access maintained under strict two person control, and the information deleted from the online system. Depending upon whether the system supports residual information protection and at what level of granularity, simple deletion may not be sufficient; erasure using commercial or custom products may be required.

Much of this information can also be protected using cryptographic mechanisms such as encryption. Such protection is of limited value in scenarios where decryption keys are stored with, or under the same controls as the information in question. These mechanisms are most effective when the information is stored on or transported to other media, and the decryption keys or the materials required to activate those keys are retained in a separate and secure place.

Given current COTS capabilities, system administrators are likely to have access to all of the information discussed above. One method mitigating the threat of administrative abuse is to provide for multi-person physical control to the system and administrative functions. Multi-person administrative control can be achieved either by permitting administrative functions from the system console or from a workstation that is under the same multi-person physical control and has the following additional security controls:

1. The remote workstation has the same computer security controls as the voting system
2. The remote workstation is connected to no other networks but the voting system and uses FIPS validated, 112 bit security FIPS algorithms, Internet approved protocols (e.g., TLS, IPSec, etc.) to secure the communication channel between the remote workstation and the voting system.
3. The communication protocol used provides for mutual authentication, integrity and confidentiality.

At a minimum, the event logs should be protected using the operating system DAC facilities.

Where applicable and feasible, the event logs should be protected using the application DAC[5].

Passwords need not be stored in the clear. Passwords should be stored in one-way encrypted form (e.g., fixed value encrypted with the password or hashed password) so that they cannot be deciphered even by the administrators. However, even if the passwords are stored in non-decipherable form, they must be protected using the operating system DAC so that no one can read the password. Users should be able to modify their own passwords using the operating system or application facilities. In addition, when applicable and feasible, application passwords should be protected using application DAC capabilities.

Secret and private keys should be protected in the FIPS 140-2 validated cryptographic modules. When the module is software based, the keys should be protected by the underlying operating system DAC. In addition, when applicable and feasible, application keys should be protected using application DAC capabilities.

3.5 Integrity

If integrity of information is not protected, it can lead to compromise of voting system. For example, unauthorized modification of stored PII can lead to an unauthorized person casting a vote. Modification to the event log can aid an

[5] For example, the operating system generated event log and RDBMS generated event log are protected by the operating system DAC. In addition, the RDBMS event log is protected by the RDBMS DAC.

attacker in covering his tracks. Unauthorized modification to system files or data can lead to the compromise of PII as well as the entire election; an attacker could undermine the election outcome. Unauthorized modification to passwords or keys can lead to the compromise of the authentication mechanism which in turn can lead to threats listed in Section 3.1.

The guidance in this section is primarily intended for voting system designers.

Table 7: Threats to Integrity

Threat to Integrity	Threat Mitigation Mechanisms
Information can be modified during transit	Cryptographically protect the information using FIPS validated algorithm using appropriate key size so that the receiving end can verify the integrity of information. Examples of cryptographic integrity protection are digital signatures, HMAC, or CMAC Physically carry the information or send it via physically protected paper mail.
Information can be modified by an attacker from a computer system where it is stored	Use a mix of computer security controls, firewalls, and IDS/IPS to deny attackers access to the information. Store the information on non-rewritable media (e.g., WORM)
Information can be modified by an unauthorized user of a computer system where it is stored	Use a mix of computer security controls provided by a secure operating system that requires identification and authentication, and provides access control mechanisms. Use the access control mechanisms of the secure operating system to restrict access to the information. Set the access controls on the information to prohibit modification. Store the information on non-rewritable media (e.g., WORM)
Stored information can be inappropriately modified by authorized personnel	Use a mix of computer security controls provided by a secure operating system that requires identification and authentication, and provides access control mechanisms. Use the access control mechanisms of the secure operating system to restrict access to the information. Use the access control mechanisms to restrict PII modification to administrators. Require multi-person control for access to administrative accounts. Store the information on non-rewritable media (e.g., WORM)

The following subsections discuss integrity-related topics:

1. Information Requiring Integrity Protection
2. Integrity Mechanisms for Information in Transit
3. Integrity Mechanisms for Information in Storage

3.5.1 Information Requiring Integrity Protection

The following are examples of information that require integrity protection:

1) PII as discussed in Section 3.3.1.
2) Ballot tracking information
3) Flags indicating whether an individual has voted or not.
4) Cast vote records.
5) Ballot/Election definition files.
6) Unmarked ballots.

7) Event logs (event logs may contain information that can be used to make inferences about voter activities).
8) All executable files.
9) All system data.
10) Passwords.
11) All cryptographic keys (private, secret and public keys).

3.5.2 Best Practices for Integrity Protection of Information in Transit

Information requiring integrity protection which is electronically transmitted should be secured using FIPS 140-2 validated cryptography, using FIPS algorithms, 112 bit security, and standardized Internet protocols. Examples of such mechanisms include:

1. TLS that is based on 2048 bit RSA certificates, using 3 key TDES and SHA-1 based HMAC[6]. SHA-1 based HMAC is applied to each packet, providing integrity to the packet and hence the data stream. HMAC secret key is securely established during the TLS.
2. IPSec that is based on 3 key TDES or AES encryption, 2048 DH Group for key exchange, and 2048 bit RSA for end-point authentication. Authentication Header (AH) is associated with each packet providing integrity. AH is calculated using either TDES CBC mode CMAC, SHA-1 based HMAC or AES CCM mode CMAC. DH is used to negotiate shared session key. The shared session key in turn is used CMAC.

The information listed in Section 3.5.1 in transit physically should be secured using continuously tracked mail; regular mail does not offer sufficient assurance of integrity.

3.5.3 Best Practices for Integrity Protection of Information in Storage

Information requiring integrity protection should be only provided to the voter and other authorized individuals.

Information requiring integrity protection should be protected from unauthorized modification while it is stored in the voting system. At a minimum, the native operating system DAC mechanism should be used to protect the voter information storage container (e.g., file or database). These protection mechanisms should only permit authorized voting system applications modify access to the voter database. Additional application level DAC should be implemented so that only authorized users whose identity has been properly authenticated can modify the voter information as described below. An example is the implementation of an RDBMS that offers fine grained DAC based on tables, rows, columns, and views. The user authentication can be obtained from the underlying operating system or the RDBMS can perform its own authentication. The user role is derived from the authenticated identity.

1. Certain records should only be modifiable by the user that owns them or an authorized authority acting on that user's behalf.
2. Other records should only be viewable by privileged roles, and then only at certain times.
3. Some records should not be modifiable under any circumstances.
4. Event logs (both the operating system and application) should not be modified by anyone except the operating system and application logging software.
    a) At a minimum, the event log integrity should be protected using the operating system DAC.
    b) Where applicable and feasible, the event log integrity should be protected using the application DAC[7].

Much of this information can also be protected using cryptographic mechanisms such as digital signatures, Message Authentication Code (MAC), HMAC, and hash. However, none of these mechanisms alone can protect the integrity of information while it is stored on the system since the adversary who can access the stored information can also access the keys to recalculate and update the integrity check. However, these mechanisms are useful when the information is stored or transported to other media and the integrity check parameters (e.g., public key, MAC or HMAC secret, or hash) are retained in a secure place.

[6] SHA-1-based HMAC is considered to offer security commensurate with the key size as opposed to 80 bits.

[7] For example, the operating system generated event log and RDBMS generated event log are protected by the operating system DAC. In addition, the RDBMS event log is protected by the RDBMS DAC.

Given the current capabilities of COTS, system administrators are likely to have access to all the information discussed above. The cost-effective way to ensure that the systems are implemented using commercial technology and protected from administrative abuse is to provide for multi-person physical control to the system and administrative functions. Note that multi-person administrative control can be achieved either by permitting administrative functions from the system console or from a workstation that is under the same multi-person physical control and has the following additional security controls:

1. The remote workstation has the same computer security controls as the voting system
2. The remote workstation is connected to no other networks but the voting system and uses FIPS validated, 112 bit security FIPS algorithms, standardized Internet protocols (e.g., TLS, IPSec, etc.) to secure the communication channel between the remote workstation and the voting system.
3. The communication protocol used provides for mutual authentication, integrity and confidentiality.

3.6 Availability

Successful denial of service attacks can prevent certain voters from being able to cast their ballots, which in turn can unduly impact the outcome of the election.

Table 8: Threats to Availability

Threat to Availability	Threat Mitigation Mechanisms
Natural Disaster such as fire, flood, earthquake	Use multiple sites. Fireproof site and computer room. Build site in area which is not in earthquake or flood zone. Computer room on upper floors. Install computers on raised floor and in racks.
Power Outage	Use multiple sites Use backup power (e.g., oil or gas operated generator)
Network Outage	Use multiple sites Procure redundant communication service from different service providers
Excessive Workload	Use multiple systems in load balanced configuration
Hardware Failure	Use multiple systems in load balanced configuration
Software or Data Loss	Perform frequent system backups
Denial of Service Attack	Use packet filters, firewalls and IDS/IPS to thwart attacks. Use capabilities of firewall and IDS/IPS to detect and anticipate denial of service attacks.

The guidance in this section is primarily intended for voting system designers.

The voting system data and functions will require high availability during the voting period. Denial of service attacks can compromise the voting functions. Two approaches are taken to ensure availability:

1. System Data Backup: Under this approach system data and files are backed up so that the system can be restored from data or file corruption; and/or
2. System Redundancy: Under this approach a hot, warm, or cold backup is available to take over if and when the system goes down.

These approaches are further described in the sections below.

3.6.1 System Data Backup

System data should be routinely backed up so that in case of system failure or data corruption, the backup can be used to restore the system. It is a good practice to perform incremental backup daily and full backup weekly.

In order to protect the integrity, confidentiality and availability of the data on the system, the backup media should be under the same multi-person system administrator control as most sensitive components of the voting system itself. See Section 6.2 for a description of additional operational controls which apply to the backup media.

Backups may be performed using one of the following mechanisms:

1. Local storage media such as tapes, Digital Video Disc (DVD), and Compact Disc (CD)
2. Backup to a central system over the communication line
3. Storage Area Network (SAN)

When backup data is sent over a communication line (e.g., for central backup or SAN synchronization) outside the secure Local Area Network (LAN), the following should be ensured to protect the data in transit:

1. FIPS validated cryptographic modules should be used
2. FIPS algorithms should be used
3. All cryptographic modules should use at least 112-bit security algorithms
4. Both ends of the communication should authenticate each other
5. Information should have confidentiality protection
6. Information should have integrity protection
7. Information should have anti-replay protection
8. Cryptographic protocol should be Internet standard

Client authenticated TLS with 2048 bit RSA certificates, 3 key TDES and SHA-1 is an example of the protocol that meets the above requirements.

Media that stores backup data should be maintained using operational controls equivalent to those used for media that stores live data, as described in section 6.

3.6.2 System Redundancy

The IT infrastructure used to support UOCAVA voting may contain redundant systems. If one system fails, the other system can take over. The redundant system can be any one of the following:

1. **Hot:** In this case, one or more systems share the operational workload with the primary system. In the case of the primary system failure, other system(s) take over. Generally, work is distributed across systems using load balancing hardware.
2. **Warm Standby:** In this case, a standby system is running and kept synchronized with the primary system. When the primary system goes down, the standby system takes over using automated detection or manual configuration.
3. **Cold Standby:** In this case, a standby system is powered down and requires manual configuration including loading the system backup tapes to bring up and operate the standby system.

In addition to redundancy within the design of the system itself, redundancy of hosting can provide additional robustness for functions that require continuous availability. For such systems, if the primary site can have a long term site failure due to natural disaster, power outage or communication failure, diverse sites should be used. A site is considered geographically diverse if the same incident will not cause failure at the secondary site when the primary site is hot with a failure (e.g., the two sites are not on the same weather pattern, on the same fault line, and same flood plain).

For any site, communication diversity should be achieved by procuring different communications lines from different communications service providers. The communications service providers must not share any of the following:

1. Facility
2. Communication trunks
3. Communication tail circuits
4. Communications service providers should either have backup power or should not share the same power utility provider.

When hot backup is used at geographically diverse sites, global load balancing hardware should be used to distribute the traffic among the diverse sites.

Note that all communications among the geographically diverse sites must be protected as listed in Section 3.6.1.

3.6.3 Best Practices for Availability of Functions

Some voting system functions are only used during an election cycle; high availability of the IT components that support them is only required during the election cycle. The election cycle is defined to begin with the pre-election time required to prepare the system for election and is defined to end with post election when the ballots have been counted.

During the election period, however, functions critical to the conduct of the election should be highly available.

The best practices for a voting system to provide a high degree of availability include all of the following:

1. Make sure that all software and firmware components (e.g., operating system, database, web server, applications, malware detectors) are running with the latest vendor patches.
2. Make sure that the malware detection software updates its signature database on a frequent basis (at least weekly).
3. Make sure that the malware detection software is executed on a regular basis (at least daily).
4. Make sure that all media introduced to the voting system (e.g., CD, USB, etc.) are scanned for malware.
5. Ensure that the firewalls only permit those services required to conduct the election, and any temporary ports opened for testing or other reasons are closed.
6. Ensure that the IDS/IPS execute with the latest signatures.
7. Conduct regular port scans on the system to identify open ports and available services.
8. Put an incident handling process in place as described in Section 6.9.
9. Store ballot information on Redundant Array of Inexpensive Disks (RAID) drives.
10. Use IDS/IPS to:
    a) Terminate offending sessions.
    b) Throttle bandwidth usage.
11. Use Network Behavior Analysis (NBA) IDS/IPS to identify threats that generate unusual traffic flows, such as Distributed Denial of Service (DDoS) attacks.

In addition to the above, the importance of the functionality provided by some IT systems will dictate additional redundancy to ensure continuous availability. Such systems should be hosted at facilities which provide for one or both of the following:

1. Use two or more sites for the systems. If more than one site is live, distribute traffic among the sites using geographical load balancers. Otherwise use automated or manual means to enable rapid failover from the primary site to a backup site in the event of an outage.
2. Use two or more voting systems at each site. If more than one system is live, distribute traffic between these using local load balancers. Otherwise use automated or manual means to enable rapid failover from the primary system to the backup system in the event of an outage.

3.7 Cryptographic Security

In this section we discuss the Public Key Infrastructure (PKI) Certification Authority (CA) requirements and requirements for cryptography and key management. The primary audience for this section is voting system designers.

3.7.1 Certification Authority (CA) Requirements

A PKI CA issues X.509 certificates to systems and personnel. These certificates serve to bind an asymmetric key pair to either a device or a user identity.

Although a dedicated CA could be deployed in conjunction with a voting system, it is not necessary or desirable to do so in most cases. The initial and ongoing costs associated with operating a dedicated CA are significant, both in terms of equipment and procedural overhead; these costs will not generally be offset unless the system being deployed requires an unusually large number of certificates. As long as the requirements specified in this section are met and all certificates along

with fresh revocation status information are accessible to the voting system, there is no security advantage to deploying a dedicated CA.

Most commonly, an existing enterprise or third party CA will be used to issue certificates that will be used by servers and personnel associated with the voting system.

Certificates issued to the voting system web servers and personnel should be issued by a CA that meets the following requirements:

1. The CA should perform identity proofing of the certificate applicant.
2. The CA should revoke a certificate if and only if an authorized party requests the certificate revocation.
3. Upon a certificate revocation, the CA should publish a Certificate Revocation List (CRL) in a timely fashion.
4. The CA should operate under personnel, physical, and procedural controls that are commensurate with those specified for the voting system in "Section 6 Operational Controls".
5. The CA should operate with computer security and network security controls that are commensurate with those specified for the voting system in Sections 4 and 5.
6. The CA should use FIPS 140-2 Level 3 or higher hardware cryptographic module for protection of the certificate and CRL signing private key.
7. The CA cryptographic module should be under two person control.
8. The CA should use the same private key to sign certificates and CRLs.

If a CA external to the voting system is used, its Certification Policy (CP) and Certification Practice Statement (CPS) should be examined in conjunction with the results of an independent audit to ensure that these requirements are met.

3.7.2 Certificate Checking

The voting system should perform TLS client authentication using certification path validation in full compliance with [RFC5280], including revocation checking.

The voting system should match the presented client certificate with the certificate registered for the claimant. The match should consist of the full certificate match.

The user should be advised to use a browser that performs certification path validation in compliance with [RFC5280], including revocation checking. The client browser should be configured for revocation checking. The following are examples of configuring revocation checking for two of the commonly used browsers:

- For Microsoft Internet Explorer (IE) use Tools → Internet Options → Advanced. Scroll down to "security" and check both "Check for publisher's certificate revocation" and "Check For server certificate revocation".
- For Mozilla Firefox use Tools → Options → Advanced. In the encryption tab, click "Validation" and check "Use the Online Certificate Status Protocol (OCSP)." If the voting system's PKI does not provide OCSP, administrators can click "Revocation Lists," import CRLs and check "Enable Automatic Update."

3.7.3 Cryptographic Algorithms

All cryptographic algorithms used should be FIPS approved. The algorithms and key sizes should be selected to provide 112 bit equivalent or greater security. All cryptographic modes of operations and schemes should be FIPS approved. All cryptographic algorithm implementations should undergo National Institute of Standards and Technology (NIST) Cryptographic Algorithm Validation Program (CAVP) and should receive a CAVP certificate. This ensures that the vendor's implementation conforms to the FIPS-approved security parameters and that this implementation will interoperate with others that have also been certified.

3.7.4 Cryptographic Module Engineering

All cryptographic modules should be validated to FIPS 140-2 Level 1 or higher. When cryptographic tokens are used by individuals, these should be hardware cryptographic modules and should be validated to FIPS 140-2 Level 2 or higher. CAs should use hardware cryptographic modules validated to FIPS 140-2 Level 3 or higher. All validated modules will receive a certificate from the NIST Cryptographic Module Validation Program (CMVP) and will have a published security policy. When operated in accordance with that security policy, validated modules meet the mandatory standards for the protection of sensitive data on Federal systems. Modules that have not been validated are considered to provide no protection to this data.

3.7.5 Best Practices for Managing Cryptographic Keys

The following guidelines should be used in managing long-term, static cryptographic keys. Ephemeral keys are managed in accordance with the cryptographic protocol that uses them.

1. The keys should be generated in FIPS validated cryptographic modules using FIPS approved method for the cryptographic algorithm(s) for which the key is intended.
2. The keys should be generated in the cryptographic module that is intended to use them, whenever possible and feasible. If this is not feasible, the keys should be transferred to the cryptographic module using FIPS approved methods, using FIPS approved algorithms, and using transport key sizes commensurate with the key being transported. The transfer mechanism should ensure integrity of the keys and confidentiality of the secret and private keys.
3. Cryptographic modules holding the keys should be protected at all times. Note that the cryptographic modules holding public keys also require protection to protect against substitution threat.
4. The keys should be changed every election cycle or every 3 years, whichever comes first.
5. The secret and private encryption keys used to protect stored data (as opposed to data in transit) and public key certificate, CRL, and Online Certificate Status Protocol (OCSP) signing keys should be backed up. The backup cryptographic module should meet all the security requirements of the operational cryptographic module.
6. Public keys should be archived based on the requirements to retain election information. This requirement applies to the extent that information is retained when digital signature need to be verified.
7. Private keys should be archived based on the requirements to retain election information. This requirement applies to the extent that information is retained in encrypted form and the private key is required for decryption.
8. Secret keys should be archived based on the requirements to retain election information. This requirement applies for the following:
    a) The information is retained in encrypted form and the secret key is required for decryption; or
    b) The information is retained and its integrity needs to be verified and the integrity is dependent on the secret key (e.g., HMAC or CMAC).
9. Secret and private keys should be reset to zero when no longer needed.

3.8 Communication Systems

This section is intended to provide guidance for securing external communications channels. These guidelines are intended for system administrators and system designers.

3.8.1 Email

This section was developed using NIST SP 800-45 *Guidelines on Electronic Mail Security*, [SP800-45], which should be consulted for background and additional details.

One or more dedicated platforms should be used for mail servers. The mail servers should have the following security controls:

1. The mail server should operate on a hardware platform dedicated to performing e-mail server and associated logging functions only.
2. The mail server should operate in a protected execution environment to protect itself from interference and tampering by other applications.
3. The platform should not permit any network based user login.
4. The platform should contain the minimum number of administrative accounts required for the mail server administration.
5. If the platform requires user accounts for mail access, the user accounts should not have any privileges. These should also apply to the administrators as mail recipients.
6. Administrative personnel should have separate user accounts as administrators and as mail recipients.
7. The appropriate and latest security template or hardening script should be applied to the server.

8. SMTP, Post Office Protocol (POP), and Interactive Mail Access Protocol (IMAP) service banners (and others as required) should be reconfigured so as not to report mail server and operating system type and version.
9. All dangerous or unnecessary mail commands (e.g., VRFY and EXPN) should be disabled.
10. The platform should be configured to execute the mail server application with a user account with the least privilege required.
11. The mail server application should limit user access to information that the user is authorized to access.
12. The mail server application should only write to the files and directories in areas dedicated for the mail server operational data. These areas should not include system files and mail server application files.
13. All users should be properly identified and authenticated.
14. Administrative accounts should require logon as described in Section 3.1.6. In addition, remote administration is strongly discouraged.
15. The platform should have only the mail server and associated logging applications installed.
16. Only those network services that are required for operation of the mail service should be installed and active. All other network services should be either not installed or disabled.
17. The mail server log should be protected from unauthorized examination and modification. The mail server log should be treated like the operating system log discussed in Section 5.4 to ensure that the mail server log cannot be used to compromise PII.
18. If inbound mail is required:
    a) Server-based malware scanning should be deployed.
    b) All attachments should be removed prior to delivery. If attachments absolutely must be allowed, all of the following should be done:
        i. Attachments that are known to be executable once decoded such as .exe .msi .com .mde, .cer, etc. should be deleted or quarantined.
        ii. Other attachments should be scanned for virus and harmful macros.
        iii. The maximum allowable attachment size should be determined; attachments above a certain size should be rejected.
    c) Server-based content filtering should be deployed.
    d) Appropriate bounce or non-delivery notice should be provided for rejected mail, unknown recipients, removed attachments, etc.
19. The mail server should reject mail from known blacklisted mail servers.
20. The mail server should relay mail from only known internal voting system IP addresses.
21. The mail server should relay mail from only authenticated users.
22. The mail server should abide by the following network architecture principles:
    a) The mail server should not be placed on the protected voting system sub-network unless it is further protected by a mail gateway. The mail gateway in turn should be in a DMZ protected from the Internet by a firewall.
    b) The mail server may be placed in a DMZ protected from the Internet by a firewall.

3.8.2 Fax and Telephone PBX

The guidelines listed below were developed using NIST SP-800-24, *PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does*, [SP800-24], which should be consulted for background and additional details.

The PBX should use the following security features:

1. Remote maintenance access should be normally blocked unless unattended access is required.
2. Local personnel involvement should be required to open remote maintenance ports when remote access is required for troubleshooting. Thus, remote maintenance cannot be enabled from remote location.

3. Two-factor strong authentication should be used on remote maintenance ports. For example, one factor can be a smart card or one-time password, and the other factor can be traditional password.
4. Maintenance ports should be physically protected from unauthorized access.
5. Password for Private Branch Exchange (PBX) accounts:
    a) Should be automatically generated
    b) Should be randomly generated
    c) Should have entropy of 64 bits
6. If fax line goes through PBX, it should use a dedicated line.

4 Voting System Network Protections

For the voting system, network protection should use a multi-layered approach by incorporating a firewall to prevent remote network-based attacks along with IPS/IDS for attack attempts that are not stopped at the firewall.

In architectures where the workstations used by election officials and administrators are on a separate network from the servers, the workstation network should use the same controls as the voting system network. In most cases, the controls for the workstation network can be more restrictive than those for the network that contains the servers, as the workstations will not generally require that external systems be permitted to access them over the network in order to provide voting application functionality.

The following sections describe the network security technologies.

4.1 Firewall

This section was developed using NIST SP-800-41 Revision 1, *Guidelines on Firewalls and Firewall Policy* [SP800-41], which should be consulted for background and additional details.

4.1.1 Firewall Types

Firewalls are devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures. There are several types of firewalls, each with varying capabilities to analyze network traffic and allow or block specific instances by comparing traffic characteristics to existing policies. These types are listed below:

1. Packet Filtering Firewall
2. Stateful Inspection Firewall
3. Application-Proxy Gateway
4. Circuit-Level Gateway
5. Dedicated Proxy Server

The following subsections describe each of these firewall types.

4.1.1.1 Packet Filtering Firewall

The most basic feature of a firewall is to filter the incoming and outgoing traffic based on one or more of the following:

1. Source Internet Protocol (IP) Address
2. Destination IP Address
3. Port Number
4. Direction (Inbound or Outbound)
5. Network Protocol (e.g.., Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP))

Unlike more advanced filters, packet filters do not protect the content of packets. Their access control functionality is governed by a set of directives referred to as a ruleset defined in terms of the 5-tuple listed above. Packet filtering capabilities are built into most operating systems and devices capable of routing. Firewalls that are only packet filters and provide no advanced features have two main strengths—speed and flexibility. Since packet filters seldom examine data above the network layer (with the possible exception of limited transport layer information), they can operate very quickly. And because most modern network protocols can be accommodated via the network layer and below, packet filters can be used to provide some security for nearly any type of network communication or protocol. The boundary router in the diagram below can be configured as a packet filtering firewall.

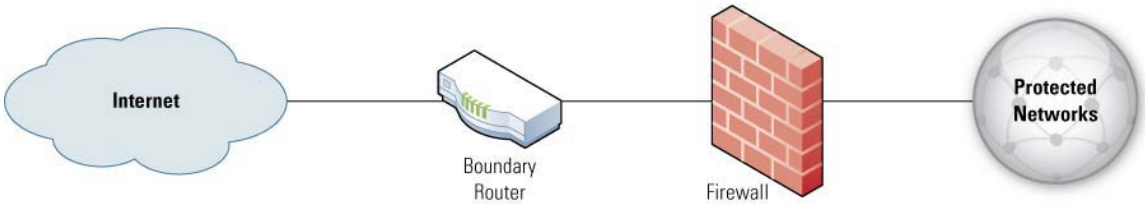


Figure 1. Boundary Router and Firewall

4.1.1.2 Stateful Inspection Firewall

Stateful inspection improves on the functions of packet filters by tracking the state of connections and blocking packets that deviate from the expected state. This is accomplished by incorporating greater awareness of the transport layer. As with packet filtering, stateful inspection intercepts packets at the network layer and inspects them to see if they are permitted by an existing firewall rule, but unlike packet filtering, stateful inspection keeps track of each connection in a state table. While the details of state table entries vary by firewall product, they typically include source IP address, destination IP address, port numbers, and connection state information. Each new packet is compared by the firewall to the firewall's state table to determine if the packet's state contradicts its expected state. For example, an attacker could generate a packet with a header indicating it is part of an established connection, in order to pass through a firewall. If the firewall uses stateful inspection, it will first verify that the packet is part of an established connection listed in the state table. A deeper inspection of the packet may also be conducted. The packet can be analyzed at the network, transport, and application protocol layers to compare firewall-configured profiles of benign protocol activity against observed events to identify deviations. This enables the identification of unexpected sequences of packets, such as issuing the same command repeatedly or issuing a command that was not preceded by another command on which it is dependent. These suspicious commands often originate from buffer overflow attacks, Denial of Service (DoS) attacks, malware, and other forms of attack carried out within. Another common feature is reasonableness checks for individual commands, such as minimum and maximum lengths for arguments. For example, a username argument with a length of 1000 characters is suspicious—even more so if it contains binary data.

4.1.1.3 Application-Proxy Gateways

An application-proxy gateway combines lower layer access control with upper layer functionality. These firewalls contain a proxy agent that acts as an intermediary between two hosts that attempt to establish communications with each other, and never allows a direct connection between the two hosts. Each successful connection attempt actually results in the creation of two separate connections—one between the client and the proxy server, and another between the proxy server and the true destination (shown in Figure 2). The proxy is transparent to the two hosts, and a direct connection seems to have been established. Because external hosts only communicate with the proxy agent, internal IP addresses are not made known to the outside world. The proxy agent interfaces directly with the firewall ruleset to determine whether a given piece of network traffic should be allowed to transit the firewall. In addition to the ruleset, each proxy agent has the ability to require authentication of each individual network user. This user authentication can take many forms, including user ID and password, hardware or software token, source address, and biometrics.

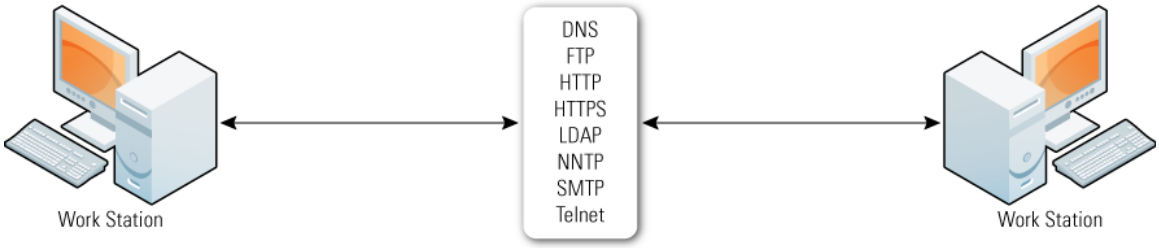


Figure 2. Proxy Gateways

The proxy gateway operates at the application layer and can inspect the actual content of the traffic. Unlike stateful protocol analysis, which mainly verifies that traffic is consistent with protocol definitions, application-proxy gateways break down the data and more thoroughly examine packet content, distinguishing between normal traffic for a specific protocol and traffic that could contain exploits for known flaws. The proxy gateways also perform the TCP handshake with the source system and are able to protect against exploitations at each step of a communication. In addition, proxy gateways can make decisions to permit or deny traffic based on information in the application protocol headers or payloads.

4.1.1.4 Circuit-Level Gateways

A circuit-level gateway is another type of proxy, and is sometimes referred to as a circuit-level proxy. In addition to their proxy capabilities, which shield internal systems from the outside world, circuit-level gateways validate each connection before it is established in a manner similar to that of stateful inspection. When a connection request is received, the circuit-level gateway checks its ruleset to determine if the connection should be allowed. In addition to the 5-tuple discussed in Section 4.1.1.1, some circuit-level gateways can also base their rulesets on user authentication or time restrictions.

Once a connection is permitted, an entry is placed in a virtual circuit table that also contains state information. Packets listed in the table are allowed to pass through the firewall without further validation. When the connection has been terminated or has been inactive for a pre-determined period of time, the entry is removed from the table. A circuit-level proxy provides many of the same features as a firewall that has stateful inspection, with the added functionality of a proxy to prevent direct connections between hosts on opposite sides of the firewall. Circuit-level gateways are usually faster than application-proxy gateway firewalls because they perform fewer evaluations on the data; they do not examine the content of the application packets.

4.1.1.5 Dedicated Proxy Servers

Dedicated proxy servers differ from application-proxy and circuit-level gateways; while they retain proxy control of traffic for one or more applications, they do not have firewalling capabilities. Although dedicated proxy servers are not firewalls, they work closely with application-proxy gateway firewalls and circuit-level gateway firewalls. Because these servers do not have firewall capabilities, they are typically deployed behind traditional firewall platforms. Typically, a main firewall could accept inbound traffic, determine which application is being targeted, and hand off traffic to the appropriate proxy server (e.g., email proxy). The dedicated proxy server would perform filtering or logging operations on the traffic, and then forward the traffic to internal systems. A proxy server could also accept outbound traffic directly from internal systems, filter or log the traffic, and pass it to the firewall for outbound delivery. An example of this is an HTTP proxy deployed behind the firewall; users would need to connect to this proxy en route to connecting to external Web servers. Dedicated proxy servers are generally used to decrease firewall workload and conduct specialized filtering and logging that might be difficult to perform on the firewall itself.

The inbound proxy servers are not used because these proxy servers must mimic the capabilities of the real server that they are protecting, an activity which becomes nearly impossible when protecting a server with many features. Using a proxy server with fewer capabilities than the server it is protecting renders the non-matched capabilities unusable. Additionally, the essential features that inbound proxy servers should have (logging, access control, and so on) are usually built into the real servers. Most proxy servers now in use are outbound proxy servers, with the most common being HTTP proxies. The figure below illustrates a typical network architecture where a DMZ is protected from the Internet using a filtering router, the Demilitarized Zone (DMZ) contains dedicated proxy servers for HTTP and SMTP and the Intranet is further protected using a stateful inspection firewall.

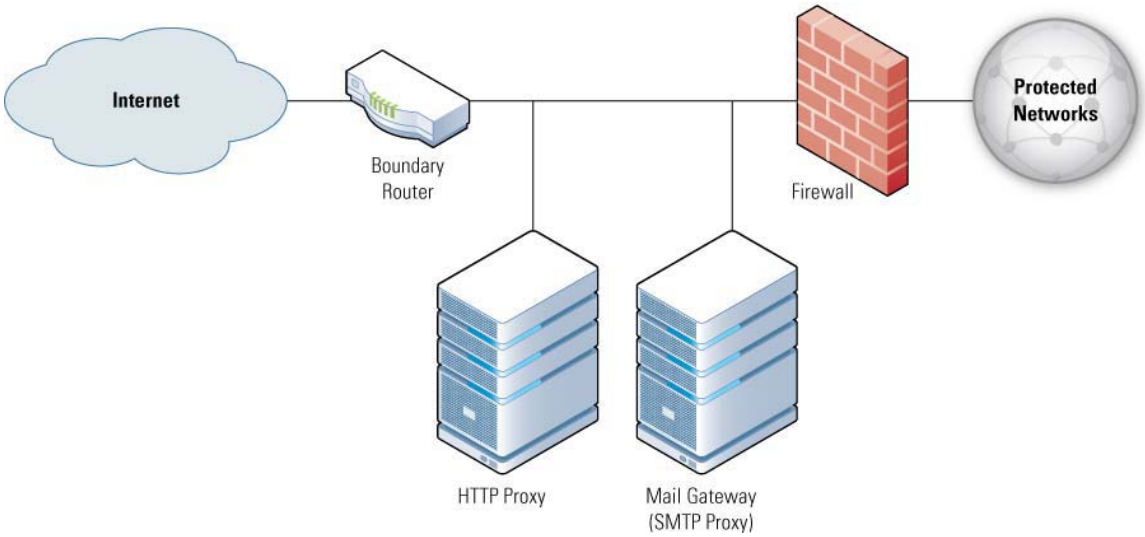


Figure 3. Dedicated Proxy Servers

4.1.2 Best Practices for Voting Systems

One or more dedicated firewall platforms (in addition to the host-based software firewall discussed in "Section 5.5 Host-Based Firewall") should be used. The firewall should have the following security controls:

1. The firewall should operate on a hardware appliance dedicated to performing firewall and associated logging functions only.
2. The firewall should operate in a protected execution environment to protect itself from interference and tampering by other applications.
3. The platform should not permit any network based user login.
4. The platform should contain the minimum number of administrative accounts required for the firewall administration. This can, and should, include separate administrative accounts for each individual administering the firewall. The platform should not contain any other user accounts.
5. The platform should have only the firewall and associated logging applications installed.
6. The platform should only have the network services installed and active that are required for handling the ports and protocols permitted through the firewall. All other network services should be either not installed or disabled.
7. The firewall log should be protected from unauthorized examination and modification.

The firewall may permit outbound Domain Name Service requests, and their corresponding replies, to registered, authorized and trust Domain Name Server servers. The firewall may optionally permit Network Time Protocol (NTP) outbound to a registered, authorized, and trusted time server if and only if time synchronization is done automatically.

The firewall may permit outbound SMTP from the mail server.

All other protocols should not be permitted in or out, except any other protocols required to perform election-related functions.

A recommended notional network architecture for the voting systems and workstations is described in Section 4.4.

4.2 Intrusion Detection System

This section was developed using NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems* [SP800-94], which may be consulted for background and additional details.

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Intrusion prevention is the process of performing intrusion detection

and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDS/IPS) are used for the following purposes:

1. Identifying possible security incidents
2. Logging information about security incidents
3. Attempting to stop security incidents
4. Reporting security incidents to security administrators.
5. Identifying problems with security policies
    a) Violations of the security policies
    b) Need to change security policies
    c) Deter individuals from violating security policies
6. Documenting current threats

An IDS/IPS cannot provide completely accurate detection; it generates false positives (incorrectly identifying benign activity as malicious) and false negatives (failing to identify malicious activity). Thus an IDS/IPS must be tuned so that false negatives are decreased. This may lead to increase in the false positives, which necessitates additional analysis resources to differentiate false positives from true malicious events.

The following topics are of interest for IDS/IPS:

1. IDS/IPS Detection Methods
2. IDS/IPS Technologies
3. Components of IDS/IPS
4. IDS/IPS Functions
5. Securing IDS/IPS
6. Best Practices for IDS/IPS Voting Systems

The following subsections discuss each of these topics.

4.2.1 IDS/IPS Detection Methods

An IDS/IPS uses one or more of the following detection methodologies:

1. Signature-based Detection
2. Anomaly-based Detection
3. Stateful Protocol Analysis

The following subsections describe each of these techniques.

4.2.1.1 Signature-based Detection

Signature-based detection compares known threat signatures to observed events to identify incidents. This is very effective at detecting known threats but largely ineffective at detecting unknown threats and many variants on known threats. Signature-based detection cannot track and understand the state of complex communications, so it cannot detect most attacks that comprise multiple events.

4.2.1.2 Anomaly-based Detection

Anomaly-based detection compares definitions of what activity is considered normal against observed events to identify significant deviations. This method uses profiles that are developed by monitoring the characteristics of typical activity over a period of time. The IDS/IPS then compares the characteristics of current activity to thresholds related to the profile. Anomaly-based detection methods can be very effective at detecting previously unknown threats. Common problems with anomaly-based detection are inadvertently including malicious activity within a profile, establishing profiles that are not sufficiently complex to reflect real-world computing activity, and generating many false positives.

4.2.1.3 Stateful Protocol Analysis

Stateful protocol analysis compares predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations. Unlike anomaly-based detection, which uses host or network-specific profiles, stateful protocol analysis relies on profiles that specify how particular protocols should and should not be used. Stateful protocol analysis monitors and tracks the state of protocols that have a notion of state, resulting in the detection of many attacks that other methods overlook. Problems with stateful protocol analysis include: it is often very difficult or impossible to develop completely accurate models of protocols, it is very resource-intensive, and it cannot detect attacks that do not violate the characteristics of generally acceptable protocol behavior.

4.2.2 IDS/IPS Technologies

The following are primary types of IDS/IPS technologies of interest in a voting system:

1. Network-based
2. Network Behavior Analysis (NBA)
3. Host-based

A combination of network-based and host-based IDS/IPS is needed for an effective IDS/IPS solution for voting systems. NBA technologies can also be deployed to counter DDoS attacks, worms, and other threats that NBAs are particularly good at detecting.

The following subsections describe each of these technologies.

4.2.2.1 Network-based

The network-based IPDS monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity.

Network-based IDS/IPSs cannot detect attacks within encrypted network traffic; therefore, either they should be deployed where they can monitor traffic before encryption or after decryption, or host-based IDS/IPSs should be used on endpoints to monitor unencrypted activity. Network-based IDS/IPSs are often unable to perform full analysis under high loads. Organizations with high-traffic loads should select sensors that can recognize high load conditions and either pass certain types of traffic without performing full analysis or drop low-priority traffic to reduce load, depending on the level of risk to the systems behind the firewall. Network-based IDS/IPSs are susceptible to various types of attacks, most involving large volumes of traffic. Organizations should select products that offer features designed to make them resistant to failure due to attack.

4.2.2.2 Network Behavior Analysis (NBA)

NBA IDS/IPS examines network traffic to identify threats that generate unusual traffic flows, such as DDoS attacks, scanning, and certain forms of malware.

NBA technologies are delayed in detecting attacks because of their data sources, especially when they rely on flow data from routers and other network devices. This data is often transferred to the NBA in batches from every minute to a few times an hour. Attacks that occur quickly may not be detected until they have already disrupted or damaged systems. This delay can be avoided by using sensors that do their own packet captures and analysis; however, this is much more resource-intensive than analyzing flow data. Also, a single NBA aggregator can analyze flow data from many networks, while a single sensor can generally directly monitor only a few networks at once. Therefore organizations that opt to avoid this delay by performing analysis on the sensors rather than on an aggregator might have to purchase more powerful sensors and/or more sensors.

4.2.2.3 Host-based IDS/IPS

A host-based IDS/IPS monitors the characteristics of a single host and the events occurring within that host for suspicious activity.

In host-based IDS/IPS, some detection techniques are performed only periodically, such as hourly or a few times a day, to identify events that have already happened, causing significant delay in identifying certain events. Also, many host-based IDS/IPSs forward their alert data to management servers in batches a few times an hour, which can cause delays in initiating response actions. Because host-based IDS/IPSs run agents on the hosts being monitored, they can impact host performance because of the resources the agents consume. Installing an agent can also cause conflicts with existing host security

controls, such as personal firewalls and VPN clients. Agent upgrades and some configuration changes can also necessitate rebooting the monitored hosts.

4.2.3 Components of IDS/IPS

The following are components of an IDS/IPS solution:

1. Sensors (also known as agents): Sensors monitor and analyze activity; sensors are used to monitor networks and hosts.
2. Management Servers: Management servers receive information from sensors and manage the sensors and the information received from the sensors.
3. Database Servers: Database servers are repositories for event information recorded by the sensors or agents and management servers
4. Consoles: Consoles are programs that provide interfaces for IDS/IPS users and administrators

These components can be connected to each other through an organization's standard networks or through a separate network strictly designed for security software management known as a management network. A management network helps to protect the IDS/IPS from attack and to ensure it has adequate bandwidth under adverse conditions. A virtual management network can be created using a virtual local area network (VLAN); this provides protection for IDS/IPS communications, but not as much protection as a physically separate management network could provide since the network infrastructure would be shared.

4.2.4 IDS/IPS Functions

Most IDS/IPSs can provide a wide variety of security capabilities. Some products offer information gathering capabilities, such as collecting information on hosts or networks from observed activity. IDS/IPSs also typically perform extensive logging of data related to detected events. This data can be used to confirm the validity of alerts, investigate incidents, and correlate events between the IDS/IPS and other logging sources. Generally, logs should be stored both locally and centrally to support the integrity and availability of the data.

IDS/IPSs typically offer extensive, broad detection capabilities. The types of events detected and the typical accuracy of detection vary greatly depending on the type of IDS/IPS technology. Most IDS/IPSs require at least some tuning and customization to improve their detection accuracy, usability, and effectiveness. Typically, the more powerful a product's tuning and customization capabilities are, the more its detection accuracy can be improved from the default configuration. Administrators should review tuning and customizations periodically to ensure that they are still accurate. Administrators should also ensure that any products collecting baselines for anomaly-based detection have those baselines rebuilt periodically as needed to support accurate detection.

Most IDS/IPSs offer multiple prevention capabilities; the specific capabilities vary by IDS/IPS technology type. IDS/IPSs usually allow administrators to specify the prevention capability configuration for each type of alert. This includes enabling or disabling prevention, as well as specifying which type of prevention capability should be used.

4.2.5 Securing IDS/IPS

In addition to hardening software-based IDS/IPS components and ensuring that all IDS/IPS components are fully up-to-date, administrators should perform additional actions to ensure that the IDS/IPS components themselves are secured appropriately. Examples include creating separate accounts for each IDS/IPS user and administrator, restricting network access to IDS/IPS components, and ensuring that IDS/IPS management communications are protected appropriately. All encryption used for protection should be performed using FIPS-approved encryption algorithms.

Administrators should maintain IDS/IPSs on an ongoing basis. This should include monitoring the IDS/IPS components for operational and security issues, performing regular vulnerability assessments, responding appropriately to vulnerabilities in the IDS/IPS components, and testing and deploying IDS/IPS software and signature updates. Administrators should verify the integrity of updates before applying them, because updates could have been inadvertently or intentionally altered or replaced. Administrators should test software and signature updates before applying them, except for emergency situations. Administrators should also back up configuration settings periodically and before applying software or signature updates to ensure that existing settings are not inadvertently lost.

4.2.6 Best Practices for IDS/IPS for Voting Systems

One or more dedicated platforms (also called appliances) should be used for intrusion detection and prevention. The IDS/IPS should have the following security controls:

1. The IDS/IPS should operate on a hardware appliance dedicated to performing IDS/IPS and associated logging functions only.
2. The IDS/IPS should operate in a protected execution environment to protect itself from interference and tampering by other applications.
3. The platform should not permit any network based user login.
4. The platform should contain the minimum number of administrative accounts necessary for the IDS/IPS administration. This can, and should, include separate administrative accounts for each individual administering the IDS/IPS. The platform should not contain any other user accounts.
5. The platform should have only the IDS/IPS and associated logging applications installed.
6. The platform should only have the network services installed and active required for operation of IDS/IPS. All other network services should be either not installed or disabled.
7. The IDS/IPS log should be protected from unauthorized examination and modification. The IDS/IPS log should be treated like the operating system log discussed in Section 5.4 to ensure that the IDS/IPS log cannot be used to compromise voter PII.

At a minimum network-based IDS/IPS should be used with the following capabilities:

1. Information gathering
2. Detection
3. Blacklisting
4. Passive prevention

Network architecture for IDS and IPS could be any one of the following, however, the IDS/IPS data must be managed so as to not reveal voter choices. Further discussion of these architectural choices is provided in NIST SP800-94.

1. Inline
2. Passive
3. Tap
4. Load Balance

Network IDS and IPS should be able to at a minimum terminate an offending TCP session. Other actions maybe also be used: firewalling (i.e., drop or reject suspicious network activity); throttling bandwidth usage; and sanitizing packets to remove malicious content.

Network IDS and IPS may optionally perform NBA, which examines network traffic to identify threats that generate unusual traffic flows, such as DDoS attacks, certain forms of malware (e.g., worms, backdoors), and policy violations (e.g., a client system providing network services to other systems).

4.3 Virtual Private Network (VPN)

A VPN encrypts traffic and provides user authentication and integrity checking and thus providing secure network links across untrusted networks. VPN technology is widely used to extend the protected network of a multi-site organization across the Internet. VPN technology is also used to provide secure remote user access to internal organizational networks via the Internet.

The following circumstances are examples of when VPN technology is used:

1. The organization wishes to secure communication between two sites without going through the cost and inconvenience of providing cryptographic capability for each user and/or machine.
2. The organization wishes to technically enforce the security policy to protect information between two or more sites
3. The organization is concerned that users may accidentally or intentionally not encrypt data sent between two or more sites.
4. Remote users and offices are connected with the location where IT systems and applications reside.

VPNs allow the firewall administrator to decide which users have access to which network resources. This access control is normally on a per-user basis; that is, the VPN policy outlines which users are authorized to access which resources. VPNs

generally rely on authentication protocols such as Remote Authentication Dial In User Service (RADIUS) [RFC2865]. RADIUS uses several different types of authentication credentials, with the most common examples being username and password, digital signatures, and hardware tokens.

Two common choices for secure VPNs are:

1. IPsec based VPN
2. TLS based tunnel VPN. TLS based tunnel VPNs can be invoked using one of the three methods
    a) Preinstalled client: This approach is most secure and recommended
    b) Downloadable client from the VPN Server: While the downloaded code is digitally signed and can be verified, the number of trust anchors in a typical workstation environment and effort required to determine true identity of signer and validity of signature make this option less attractive. Additionally, the user must have sufficient privileges to install the downloaded client.
    c) Java applet download: While the downloaded code is digitally signed and can be verified, the number of trust anchors in a typical workstation environment and effort required to determine true identity of signer and validity of signature make this option less attractive.

The three most common VPN architectures are:

1. Gateway-to-Gateway
2. Host-to-Gateway
3. Host-to-Host

The following subsections describe each of the architectures:

4.3.1 Gateway-to-Gateway

A gateway-to-gateway VPN connects multiple fixed sites over unsecured network (e.g., the Internet) through the use of a VPN gateway. This architecture is used to connect geographically dispersed offices of an organization. A VPN gateway is usually part of another network device such as a firewall or router. When a VPN connection is established between the two gateways, users at the two locations are unaware of the connection and do not require any special settings on their computers.

The advantage of this approach is that it is cost-effective and enforces the security policy for protection of data in transit. However, this approach does not protect users within the protected Enterprise network from each other or protect sensitive hosts and servers from internal users.

4.3.2 Host-to-Gateway

A host-to-gateway VPN provides a secure connection to the network for individual remote users, who are located outside the physical network. In this situation, a client on the user machine negotiates the secure connection with the VPN gateway. The gateway side of the Host-to-gateway VPN is part of the firewall.

The advantage of this approach is that is very useful for telecommuters and travelers to electronically connect to the office and access all the resources. The disadvantage of this approach is that is requires each remote user to install the VPN client. The host to gateway VPN client can also provide an attack path if the remote machine is connected on an unsecured network. An attacker can compromise the machine over the unsecured network and then use the machine to attack the organization's network.

4.3.3 Host-to-Host VPN

Host-to-host VPN is rarely used. This setup typically enables remote administration of a single server.

The advantage of this approach is that two highly sensitive hosts located in different locations can securely communicate with each other.

4.4 Log Management Infrastructure

Because of the sensitivity of the information likely to be contained within UOCAVA system and network logs, UOCAVA systems should not share an organization-wide centralized log management infrastructure. Because the log entries themselves are potentially sensitive, any centralized log repository receiving data from the system should be protected using the same controls as the information on the most sensitive hosts from which it receives log data.

In determining whether or not a centralized log management infrastructure is required for a UOCAVA system, the size and purpose of the deployment should be taken into consideration. Copying logs to a centralized, distinct system provides valuable assurance that the logs constitute an accurate record of system activities. It also streamlines log review during operation. Because of the verbosity of the log entries on systems configured according to the guidelines in this document, when centralized log management is implemented, a dedicated logging network may be required in order to prevent the increase in network traffic from interfering with the operation of the system.

The size and scope of many installations will be sufficiently limited that the processes and policies outlined elsewhere for log management and processing can be followed for each host and component of the system without imposing prohibitive personnel overhead, and other controls may provide assurance that logs are accurate.

If the scale or function of a particular deployment requires centralized log management, designers and administrators should consult NIST SP 800-92, *Guide to Computer Security Log Management* [SP800-92], for detailed guidance on the design and deployment of a secure, dedicated log management infrastructure specific to the voting system. The controls in this publication should be applied to any such system.

4.5 Best Practices for Voting System: Network Architecture

The figure below depicts a network architecture which follows the best practices described in this document for an IT system used to support UOCAVA voting.

The architecture has the following salient features:

1. The voting system and administrative consoles are within a physically secure environment.
2. The administrative consoles are directly connected to the voting systems.
3. The voting system is under two person physical control.
4. The voting system is protected by a stateful inspection firewall.
5. The DMZ is protected by filtering router.
6. The DMZ contains outbound proxy for SMTP and HTTP.
7. Network-based and host-based IDS/IPS are installed on the voting system network and servers respectively.
8. The election official workstations are within a physically secure environment.
9. The election official workstations are connected by Host-Gateway VPN to the voting system.
10. The election official workstations are protected by Enterprise firewall.
11. Host-based IDS/IPSs are installed on the election official workstations.

In the diagram, it is assumed that system administration is conducted within the application hosting facility, while election officials configure the application to support a particular election from a separate location, designated an “Election Management Facility” on the diagram.

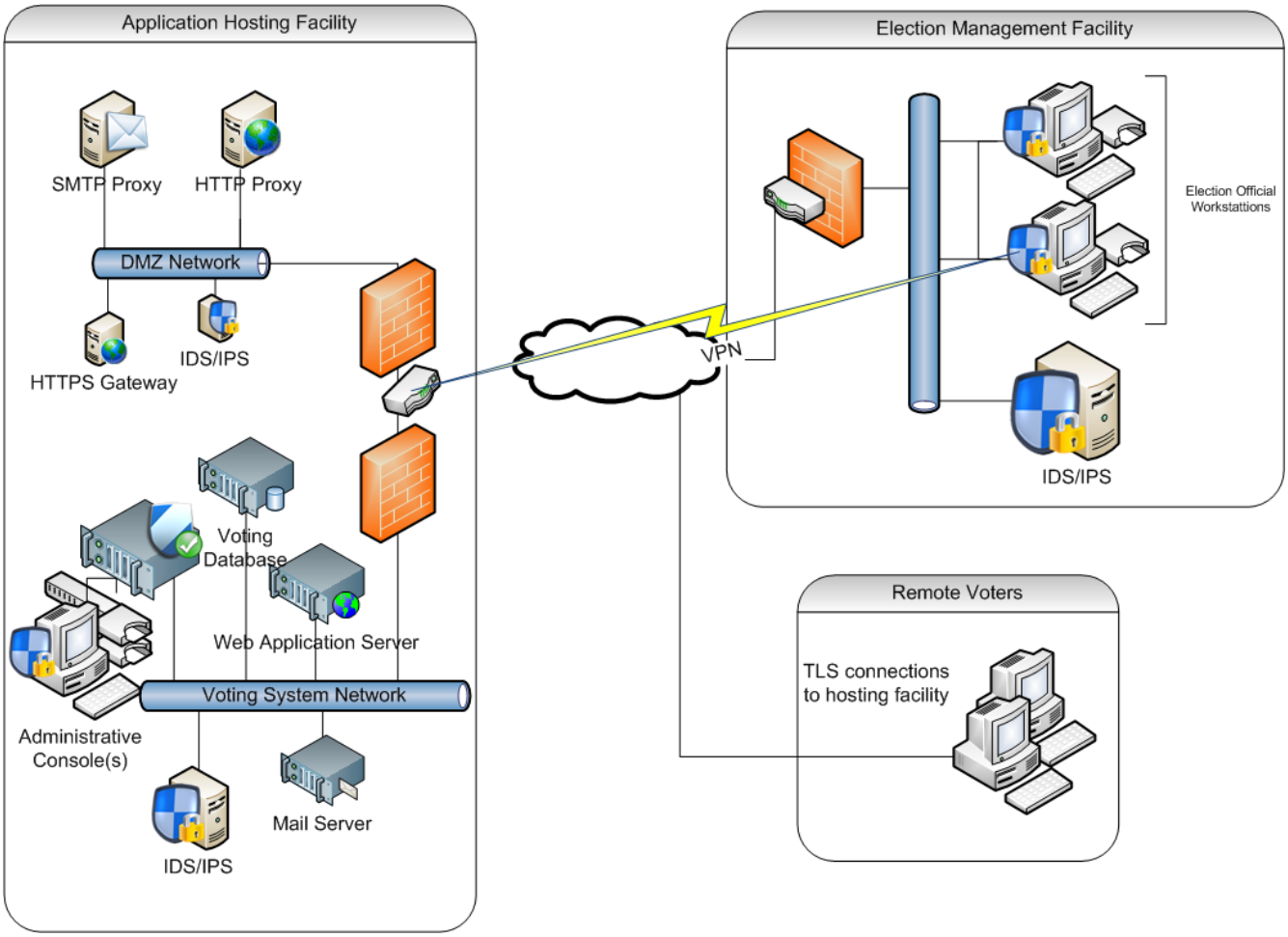


Figure 4. Voting System Network Architecture

5 Host Protection

All servers and workstations that provide IT services in support of an overseas voting system should be protected using appropriate system and application security controls. The specific mechanisms and settings involved will differ according to the purpose of the server or workstation in question. This section outlines controls and practices that should be configured on every system. For detailed configuration steps and additional, application-specific considerations, consult the National Checklist Program (http://checklists.nist.gov) as well as application-specific NIST guidelines published on http://csrc.nist.gov/.

Although much of the information in this section will be useful to system designers, the guidelines here are primarily intended to be used by voting system administrators to deploy overseas voting systems securely.

For each server and workstation, the protections specified in the following subsections should be used to establish a secure baseline configuration. The function of each system should be clearly defined, and the most restrictive protections which will permit fulfillment of that function should be selected in each area.

Once the systems are configured and brought into operation, the configuration management guidance outlined in Section 6.6 should be followed to ensure their continued secure operation

This baseline should be documented prior to the deployment of each server or workstation and kept up-to-date as changes are made. The controls described in section 6.6 should be used to ensure that the secure baseline configuration is continuously updated.

5.1 Operating System Identification & Authentication (I&A)

The operating system I&A is used to authenticate individuals who are required to use the operating system. There is no need for accounts other than administrative users for the operating system accounts. Election officials and voters obtain services via voting application and thus do not require operating system accounts.

Identification and authentication of administrative personnel to the operating system should be user ID and password or certificate based as discussed in Section 3.1.6.

5.2 Operating System Discretionary Access Control

The Operating System DAC should be used to protect all the system and voting application files. Only users and processes that require access to system and voting application files should be granted access to those files. Additionally, only the required level of access permissions (e.g., read, write, execute) should be granted. All other users and processes should not have access to those files.

5.3 Account Management

Server and workstation operating systems should be configured such that only the authorized administrators can create accounts on the system. On servers, aside from the authorized administrators, voting applications may need accounts in order to execute with application account privileges as opposed to administrative privileges. This approach helps enforce the principle of least privilege.

Servers should only contain the accounts that are required for the operation of the system. Furthermore, the accounts that do not require operating system logon should be configured to prohibit logon.

On workstations, aside from the system administrator, the workstation should only contain the accounts for the voting system administrators or the election officials who use the workstation to access the voting system.

See http://checklists.nist.gov/ for detailed guidance on configuration of specific systems.

5.4 Event Log

The operating system event logs should be protected from unauthorized examination and modification using operating system DAC as described earlier.

System clocks should be synchronized with an authoritative time source using NTP. System clock synchronization against a time source is required to ensure that the analysis of event ordering and timing is accurate.

The following list of events should be logged by the operating system:

1. System startup
2. System shutdown
3. Login and logout
4. Execution of applications and services
5. Administrative actions
6. Changes to system configuration
7. Change in authentication values (e.g., password, certificate)
8. Event log
    a) Change to list of events to be logged
    b) Event log deletion
    c) Overwrite of event log
    d) Backup of event log
    e) Change in event log space allocation (e.g. log roll threshold, maximum log size)
    f) Change to system clock
9. Modification to system files
10. Addition and deletion of files
11. Backup
12. Restore
13. Unsuccessful attempts to access any file
14. Any attempt to access system files
15. Account Management
    a) Creation
    b) Deletion
    c) Modification
    d) Changes to privileges
16. Malware protection software events
    a) Software update
    b) Signature update
    c) Execution
17. Cryptographic key generation and destruction: This event may be generated manually, by the operating system or cryptographic module.

5.5 Host-Based Firewall

Voting system servers and workstations should be configured with a host-based firewall.

The firewall should be configured to allow only the minimum set of inbound and outbound connections required for the operation of the voting application. These connections should be limited to protocols and IP addresses designated as narrowly as possible.

Consult http://checklists.nist.gov/ for specific guidance on host-based firewall configuration.

5.6 Minimize Services

Servers and workstations should be configured such that the network services and other computing services software that are not required for the operation of the voting application are removed from the system altogether. If they cannot be

removed, execution of these services should be disabled. Auto-run and auto-play upon introduction of media and files in the system should be disabled.

Note that a locked down and secured voting system will have many otherwise routine network and computing services removed and disabled. Unless necessary for a system to perform its duties, the following services should be disabled or removed on both servers and workstations:

1. File and printer sharing services (e.g., Windows Network Basic Input/Output System (NetBIOS) file and printer sharing, Network File System (NFS)], File Transfer Protocol (FTP))
2. Wireless networking services
3. Remote control and remote access programs
4. Directory services (e.g., Lightweight Directory Access Protocol [LDAP], Network Information System [NIS])
5. Email services (e.g., Simple Mail Transfer Protocol (SMTP[8]))
6. Language compilers and libraries
7. System development tools
8. System and network management tools and utilities, including Simple Network Management Protocol (SNMP).

5.7 Host Based Intrusion Detection and Prevention

Each server and workstation should contain and operate a host based intrusion detection and prevention system. At a minimum, the tool should detect and prevent modification of all executable files and addition of any executable files. It should detect and prevent attempts to modify system files. The tool should monitor for and alert administrators to modification of access rights to key system files.

Consult http://checklists.nist.gov for detailed guidance on configuration of host-based intrusion prevention systems for specific operating systems.

5.8 Malware Protection

Each server and workstation should be configured with malware protection that can detect viruses, Trojans, worms, spyware and rootkits. The malware protection software should be configured for the following:

1. Regular periodic scan
2. Scan removable media
3. Real-time on-access file scanning

On hosts where real-time on-access file scanning interferes with the voting application, real-time scans of newly created files may be configured instead of full on-access scanning.

5.9 Backup and Restore

The system should provide backup and restore capabilities for all servers. If the backup and restore functions provide cryptographic checksum (e.g., digital signature, MAC, HMAC, or hash) protection, the protection should be enabled and configured. The checksum should be stored separately from the backup media. Prior to restoring the server from the backup media, operators should confirm the integrity of the backups using the checksum.

Workstations may not require backup and restore capabilities if they do not store critical data for the voting system.

5.10 Voting System Application Security

In order to support the functions performed by the election officials and voters, voting systems will require applications. Examples of the applications include: Web Server, Web Server Application, DBMS, and DBMS applications.

The following subsections describe application level security controls.

[8] This capability may be required if the application uses automated e-mail as the mechanism to provide ballots.

5.10.1 Application Level Identification & Authentication

The application level I&A is used to authenticate individuals who require use of the application. Examples include voters and election officials. They are likely to be authenticated to the Web based application using the means described in Section 3.1.6

5.10.2 Application Discretionary Access Control

The application DAC should be used to protect all voting application data. The application DAC should permit the election officials and voters to perform their functions under the control of the application only. Role based access control is well-suited for application level DAC for voting system applications. In most situations, the voting system designer should be able to implement role based access control using group or role mechanism provided by the application or the underlying operating system.

5.10.3 Application Account Management

The application should be configured such that only the authorized administrators can create application accounts. The accounts may be required for the election officials. See http://checklists.nist.gov/ for detailed guidance on configuration of specific operating systems.

5.10.4 Application Event Log

The application event logs should be protected from unauthorized examination and modification using operating system DAC.

Where feasible, the application event logs should also be protected from unauthorized examination and modification using application-enforced DAC.

See section 3 for a discussion of the use of DAC to counter threats confidentiality and integrity.

The application event logs should use the operating system clock for time stamping the events.

The following list of events should be logged by the application:

1. Application startup
2. Application shutdown
3. Login and logout
4. Administrative actions
5. Changes to application configuration
6. Changes to ballot configuration
7. Change in authentication values (e.g., password, certificate)
8. Event log
    a) Change to list of events to be logged
    b) Event log deletion
    c) Overwrite of event log
    d) Backup of event log
    e) Change in event log space allocation (e.g. log roll threshold, maximum log size)
9. Account Management
    a) Creation
    b) Deletion
    c) Modification
    d) Changes to privileges
10. All ballots generated, excluding ballot number

5.10.5 General Application Security Practices

Voting system applications should be designed and implemented using the following principles:

1. Applications should be developed using a well-understood coding convention.
2. No operating system "system files" should be accessed.
3. Applications should not execute with impersonation (e.g., impersonation in Windows and SUID in Unix).
4. Applications should not interact with other applications.
5. When accessing a system object, its full path name should be used. This protects against path variable related errors as well as malicious attempts to subvert the system.
6. Use of hard or symbolic links (e.g., shortcuts for Windows) should be disabled.
7. All executable files should be placed in a folder that does not have the modify permission for anyone.
8. All user input should be validated.
9. Protection against buffer overflows and memory leaks should be provided.
10. No services should be provided until the user is properly authenticated.
11. No third-party scripts or executable code should be used without verifying the source code.

Additionally, vulnerability analysis and remediation should be performed and documented as described in Section 7.2.

5.10.6 Web Application Security Practices

This section was developed using NIST SP 800-44 Version 2, Guidelines on Securing Public Web Servers [SP800-44], and NIST SP 800-123, Guide *to General Server Security* [SP800-123]. Readers may consult these documents for background and additional details.

Web-based voting applications should be designed and implemented using the following principles:

1. All the principles listed in Section 5.10.5.
2. The system should include protection mechanisms against web bots.
3. A single hard drive or logical partition should be dedicated for Web content. Furthermore,
    a) This drive/partition should not contain any other information.
    b) All directories and subdirectories in this drive/partition should be exclusively for Web server content files, including graphics but excluding scripts and other programs
4. A single directory should be used exclusively for all external scripts or programs executed as part of Web server content (e.g., Common Gateway Interface (CGI), Active Server Pages (ASP)). This directory should not contain anything except external scripts or programs, and the web server should not be configured to execute scripts or programs located elsewhere.
5. A complete Web content access matrix should be developed that identifies which directories and files within the Web server document directory are restricted and which are accessible (and by whom).
6. Directory listings by the web users should be disabled.
7. Execution of scripts that are not exclusively under the control of administrative accounts should be disabled. This action is accomplished by creating and controlling access to the separate directory intended to contain authorized scripts.
8. Server Side Includes (SSI), or their execution, should be disabled.
9. Web content generation code should be scanned or audited.
10. No process except web server administration processes should be able to write to web content files. This can be accomplished by using the operating system discretionary access controls on the web content files and directories.
11. Dynamically generated pages should not contain dangerous metacharacters (e.g., & ; ` ' \ " | * ? ~ < > ^ ( ) [ ] { } $ \n \r\0)
12. Character set encoding should be explicitly set in each page.

13. Special characters or HTML tags should be processed so that they cannot be used for exploitation.
14. Cookies should be examined to ensure they do not contain any unexpected data.
15. Input validation should be performed by the web application so that the web application's security mechanisms cannot be bypassed when a malicious user tampers with data he or she sends to the application, including Hypertext Transfer Protocol (HTTP) requests, headers, query strings, cookies, form fields, and hidden fields. This mechanism also protects against Cross-Site Scripting (XSS) and Structured Query Language (SQL) injection attacks.
16. In many cases, there should not be a need to permit the users to upload files to the Web Server. If such a need were determined,
    a) Uploads should not be readable by the Web server. This can be accomplished by using the operating system discretionary access controls on upload files and directories.
    b) Uploads should be limited to a defined directory. The directory and its subfolders should not be readable by the Web server.
17. All sample scripts should be removed from the operational system.
18. Cross Site Request Forgery (CSRF) attacks should be prevented by making sure that neither an attacker nor a script running on the attacker's website has sufficient information to construct a valid request authorizing an action (with significant consequences). This can be done by inserting unpredictable challenge tokens associated with the user session into each request into URLs or forms that cause actions to be performed on behalf of the user.
19. The web application should be protected against TLS renegotiation attacks. The TLS renegotiation extension protects against these attacks. In lieu of, or in addition to, the use of TLS renegotiation extension, web pages and applications should be designed so that when a step up authentication occurs, inputs provided by the client that resulted in the need to negotiate higher authentication level are ignored and the client is required to resubmit the request after the requisite authentication is complete.
20. Follow community recommended best practices for web application development for specific languages or frameworks, e.g., .NET, PHP, Java, Ajax, etc.

Systems administrators may consult NIST SP800-44 *Guidelines on Securing Public Web Servers* for a list of tools for vulnerability scanning and log analysis.

Additionally, vulnerability analysis and remediation should be performed and documented as described in Section 7.2.

5.11 Workstation Network Protections

When workstations are on a separate network from the servers in an overseas voting system, the workstation network should be protected using similar mechanisms to the voting system network. This network protection should use a multi-layered approach by using a firewall to block remote network-based attacks as well as IPS/IDS in case some attack attempts are not stopped at the firewall.

5.11.1 Firewall

In addition to the host-based firewalls installed on each workstation, the workstation network should be protected by one or more dedicated firewalls. The requirements for the workstation network firewall are the same as those for the host network firewall, detailed in section 4.1.

5.11.2 Intrusion Detection System

In addition to the host-based IDS installed on each workstation, network-based IDS should be employed on the workstation network. The guidelines for IDS configuration detailed in section 4.2.6 also apply to the workstation network.

5.11.3 Virtual Private Network

The workstation should be connected to the voting system using the VPN detailed in Section 4.3.

6 Operational Controls

The controls described in this section apply to the voting system, firewall, IDS/IPS protecting the voting system, and mail server used for fulfilling voting system functions. As applicable, the requirements apply to the hardware, operating system software, application software, and cryptographic equipment. The guidelines in this section will be most beneficial to system administrators and technical staff charged with routine operation of UOCAVA systems.

6.1 Facility Controls

The site and room for the voting system should have the following controls:

1. The voting system site and room should have physical security controls to protect highly sensitive systems.
2. The voting system should have a reliable power source to ensure system availability commensurate with commercial systems.
3. The voting system should have reliable air conditioning to ensure system availability commensurate with commercial systems.
4. The voting system should have protections against water and fire hazards commensurate with commercial systems.

6.2 Media Storage and Off-site Backup

Media and backups should be stored in a location with controls commensurate with those specified in Section 6.1.

Media and backups should be under the same multi-person control as the live system. This may be achieved using a combination of logical and physical controls, e.g. by encrypting the backup data and storing the keys separately from the activation data needed to access them.

The system administrator should use manual or automated means to keep records of all media which are loaded with data from the voting system.

These records should be sufficiently detailed to positively identify the media.

The storage location of all media containing voting system data should be recorded.

The system administrator should use manual or automated means to record all access to the backup or archival media.

Access to media and backups should be audited using the same process and frequency as access to the live system.

When media will no longer be used to store voting system data, the media should be destroyed or sanitized in accordance with the practices defined for removal of the system from service. See Section **Error! Reference source not found.** for additional details.

6.3 Personnel Security Controls

6.3.1 Position Categorization

For the system administrator and election official positions:

1. Risk designations should be developed;
2. Screening criteria for individuals filling these positions should be developed; and
3. Individuals nominated for these positions should undergo a screening process.

6.3.2 Separation of Duties

A system administrator should not be assigned an election official role and vice versa.

Physical, technical, procedural controls should be employed such that physical and logical access to the voting system, and performance of administrative tasks requires two system administrators. Note that this may require that the administrator use local consoles only to login and perform their tasks.

6.3.3 Qualifications, Experience, and Training

The system administrators and election officials should meet the following requirements related to performance of their duties:

1. They should successfully complete an appropriate training program commensurate with their role.
2. They should have demonstrated the ability to perform their duties.
3. They should not be assigned other responsibilities that would interfere or conflict with their ability to perform their duties.

The system administrators and election officials should be provided system manuals, user manuals, and procedures required to perform their duties.

6.4 Event Log Processing

On a UOCAVA system where components have been configured in conformance with the practices described in this document, the event logs will constitute a record of all significant activity. Appropriate management and processing of these logs is important to ensure the integrity of every system function. For detailed guidance on log management, consult NIST SP 800-92, *Guide to Computer Security Log Management* [SP800-92].

6.4.1 Frequency of Event Log Processing

Event logs should be processed frequently enough that no data is lost or overwritten. During election, this may mean daily processing or more frequently; testing should be performed to establish a safe frequency.

Where possible, an automated alert should be triggered well before the event log storage becomes full so that the system administrators can back up the event log.

6.4.2 Frequency of Event Log Review

During an election, the event logs should be reviewed daily. The objective of the review should be to determine if suspicious activities are taking place and if the event log processing schedule is appropriate. Section 6.4.3 contains additional details on events to examine.

6.4.3 Vulnerability Assessments

The developer of the UOCAVA system should supply a vulnerability assessment with the system documentation. This documentation includes potential approaches that an adversary could take in an attempt to subvert or disrupt the operation of the voting system. It also includes guidance advising system operators and administrators as to how such attempts might be detected and prevented. A critical element of this is monitoring the system's event logs.

The following are typical examples of events which could indicate attempts to subvert the system:

- Excessive number of events
- Failed login attempts
- Excessive password changes to the same account in a short period of time
- Creation of accounts
- Changes to account profiles
- Account lock out events
- Gaps in event logs
- Modification of critical system files
- Read access to sensitive files
- Installation of programs
- File access failures
- Changes to audit profile
- Changes to authentication policy
- Changes to file metadata (e.g., ownership, access control list, etc.)
- All accesses to databases and files containing PII

These and similar events described in the documentation delivered with the voting system should be monitored. Consult the system documentation for additional events that are indicative of attempts to violate the voting system security.

6.5 Backup and Archive

System backups sufficient to recover from failures should be made on at least a daily basis during the election. Recovery from these backups should be tested as part of system deployment prior to the election.

Event logs should be archived for retention based on the election records retention requirements.

System backups and event logs should meet the requirements for facility security specified in Section 6.1.

Access to system backups and event logs should be under multi-person system administrator control as specified in Section 6.3.2.

6.6 Configuration Management

The configuration of the components comprising a UOCAVA system should be managed according to a formal, documented policy and procedures. The policy and procedures should be periodically reviewed to ensure that the controls established for the various components of the system are maintained when the policy is adhered to and the procedures are followed.

6.6.1 Baseline Configuration

When the components of the system are deployed, the baseline configuration should be documented. This should include all details necessary to deploy the component into the production system. When changes are made, the documentation of the baseline should be updated as part of the change management process.

Where possible, automated mechanisms (e.g., SCAP-validated scanning tools) should be used to monitor and report the configuration of each component. Any deviation from the documented secure baseline should be flagged for review, and should trigger either a change to the component's configuration or an update to that documentation.

6.6.2 Configuration Change Control

All proposed changes to the system should first be formally proposed, reviewed and approved using a change control process that meets the requirements defined in the configuration policy. This process should record the rationale for and approval of each change to the system's configuration.

Where feasible, configuration changes should be deployed using automated tools that can ensure that the changes being deployed are the same as those that have been approved.

The analysis of each proposed change should focus on ensuring that all required security controls are maintained.

After a change has been deployed, the change control process should ensure that the deployed configuration change matches the documented configuration change and that the baseline configuration is updated.

6.6.3 System Hardware and Software Inventory

The system administrator should use manual or automated means to keep records of hardware and software installed on the voting system.

The system administrator should use manual or automated means to record all events related to updates to, and the disposition of, the hardware and software.

All hardware and software should contain sufficient information for precise identification of a configuration. This may include manufacturer, make and model, version number, and revision number. Where feasible, this information should be collected, documented and monitored for changes using automated mechanisms. For an expanded list of configuration items that may apply, see NIST SP 800-40 Version 2, *Creating a Patch and Vulnerability Management Program* [SP800-40].

6.6.4 Cryptographic Material inventory

The system administrator should use manual or automated means to keep records of hardware and firmware used in cryptographic modules.

The system administrator should use manual or automated means to record all events related to updates to, or the disposition of, the cryptographic hardware and firmware.

All cryptographic hardware and firmware should contain sufficient information to identify precisely which hardware is in use at a given time. This may include manufacturer, make and model, version number, and revision number; consult the documentation supplied with the system for details.

6.7 Disaster Recovery

The voting system should contain a disaster recovery plan from various failures such as:

1. Facility unavailability
2. Cryptographic module failure
3. Hardware failure
4. Software failure

The disaster recovery plan should undergo a successful test one week prior to start of election.

6.8 Ongoing Testing

6.8.1 Penetration Testing

The voting system should undergo penetration testing after it is fully deployed to ensure that the vulnerability assessment is conducted against the exact configuration that will be used to conduct the election. This testing should take place as near to the start date of the election as is feasible, to enable the penetration testers to take advantage of the most recent known vulnerabilities, while at the same time providing system owners, administrators and vendors an opportunity to mitigate any discovered vulnerabilities. The testing should be conducted by experienced experts in penetration testing. The testers should be provided with all the system design documentation available to the voting system developer and should use information from this documentation to retrieve information on potential vulnerabilities from the National Vulnerability Database (NVD). Any vulnerability identified by the penetration testing should be resolved before the system is deemed fit for conducting the election.

See NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment* [SP800-115], for additional guidelines.

6.8.2 Network Configuration Monitoring

The voting system network configuration should be verified using the penetration testing, network mapping, and IDS/IPS tools as close to the start of the election as is feasible, allowing time for system administrators to resolve any problems that are discovered.

The voting system network configuration should be monitored on an ongoing basis by the IDS/IPS tools.

The voting system firewall rules should be examined and verified to be accurate and enforced by using the penetration testing, network mapping, and IDS/IPS tools.

6.8.3 Availability Monitoring and Load Testing

Prior to the start of the election, the voting system should be tested under anticipated peak load conditions and the response time should be verified to be within target goal. The load should be created for each class of user functions the voting system supports, i.e.

1. Registration Database Update
2. Obtain a Ballot
3. Cast a Ballot

This testing should be conducted once the projected load is known and with sufficient lead time to address concerns raised by load testing.

During the election, the voting system should be monitored using automated or manual means to ensure that all the user functions listed above are available.

6.8.4 Compliance Audit

Prior to the start of the election and in conjunction with penetration testing, the voting system should undergo a compliance audit to ensure that the voting system has controls in place to meet the requirements specified in this document. Any

deficiencies identified by the compliance audit should be corrected and an incremental audit should be conducted to ensure that all the deficiencies are closed prior to the start of election.

The audit should take place only after the final configuration has been put into place for the election. Scheduling considerations for the audit should balance the need to audit the configuration that's actually used during the election period with the need to allow enough time to address any concerns raised by the audit.

6.9 Incident Handling

The voting system operator should have incident reporting and handling systems and processes in place. These should provide the following functions:

1. There should be a mechanism for voters, election officials, and system administrators to report security incidents.
2. Reported security incidents should be kept in a secure manual or automated database.
3. Only authorized development and system administration personnel should have the ability to access the database for both review and updates
4. Each open security incident should be assigned to an individual as recorded in the database.
5. The database should maintain the status of the incident in terms of whether it is being investigated, has been confirmed, being fixed, or has been fixed.

Any problems with commercial products used in the voting system should be resolved in conjunction with the commercial product vendor in order to fix the vulnerability.

6.10 Removal from Service

Prior to removal from service or disposal of equipment, the following activities should be undertaken:

1. All cryptographic equipment should be zeroed out.
2. All event logs on the computer systems should be archived.
3. All files on the computer systems should be deleted.
4. Hard drives and other storage media used by system equipment should be sanitized before those components are disposed of or repurposed. Section 5 of NIST SP 800-88, *Guidelines for Media Sanitization* [SP800-88], contains descriptions of sanitization methods. Degaussing or destroying hard drives can provide high assurance that any sensitive data previously stored on the drive is not recoverable. If storage media will be repurposed, organizations may clear the drive by using a secure eraser tool to overwrite the hard drive with random data. For some ATA hard drives which support the Secure Erase command, a better option may be to use a tool to securely purge a drive using this special-purpose command in the ATA specification.
5. The computer system should be powered off for few minutes prior to release of the equipment.

7 Assurance Requirements

The controls described in this section apply to the servers and workstations that comprise the voting system, firewall, IDS/IPS protecting the voting system, and mail server used for fulfilling voting system functions. Where appropriate, these requirements apply to the hardware, operating system software, application software, and cryptographic equipment. The purpose of these assurance requirements is to establish confidence that the system as a whole has been both evaluated and determined to meet the security requirements of the application, and that the system is being operated in the same configuration that was evaluated.

This section should be used by system designers, both in the selection of components and as a checklist for documentation that should accompany the overall system. It should be used by personnel charged with administration and deployment of UOCAVA systems as a reference to documentation that will accompany the system. By following these guidelines, designers and implementers can ensure that the IT systems being deployed will enforce the controls discussed in previous sections.

7.1 Documentation Requirements

The documentation described in this section should be provided by the designer of each system or component and should be evaluated along with the system being deployed. Its purpose is to ensure that the system is deployed and maintained in a configuration with the same security controls as the system whose security was evaluated prior to selection.

7.1.1 Administration Guidance

The requirements specified in this section should also be applied during the selection or development of products that comprise a UOCAVA system. Each product used to support UOCAVA voting should be accompanied by detailed guidance documentation in the following areas:

1. Secure Delivery, Installation, and Start-up Guides
2. Administration Guide
3. Maintenance, Upgrade, and Flaw Remediation Procedures

This guidance should be evaluated along with the system to ensure that it is sufficient to bring the system into a secure operational state and that the configuration which results from following this guidance is identical to that which was evaluated and determined to meet the security requirements.

7.1.1.1 Secure Delivery, Installation, and Start-up Guides

All components supplied as part of a UOCAVA system should be accompanied by detailed documentation of the procedures necessary to deploy the components in the secure configuration that was used to certify their suitability for use in the voting system. These should include

- Guidance for validating the integrity of the hardware and software components that will be deployed as part of the UOCAVA system
- Documentation of the installation procedures necessary for a secure configuration
- Documentation of the procedures required to place the system in a secure operational state

The totality of this documentation should be sufficiently detailed that administrators can verify that the components being deployed are

- Complete, as selected by the system designer
- Do not differ from those that were evaluated and determined to provide the security features required by the UOCAVA system
- Configured identically to the components whose security was evaluated
- Are operating in a secure state once all components have been installed

Designers should consult [CEMv3.1] for further detail on evaluating whether component documentation is sufficient to achieve these goals.

The administrator should use the secure delivery guide to confirm the completeness and validity of all delivered system components.

The administrator should use the same secure installation and start-up procedures that were used to evaluate security as part of the system design to install the system and bring it into an operational state.

7.1.1.2 Administration Guide

Components deployed as part of a UOCAVA system should be accompanied by guidance documentation for system administrators. This documentation should describe each user role necessary for the operation of the system. The description of these roles should include the functions and privileges accessible to and required for each role and detail mechanisms for restricting them. This documentation should also explain those restrictions necessary in order to operate the UOCAVA system in a secure manner.

System designers should ensure that this guidance is clear, comprehensive and compatible with operation of all components in the context of an election. Designers should consult [CEMv3.1] for guidance on evaluating the administrative documentation that accompanies system components.

The administrator should use the administrator guidance that has been evaluated in this context to manage the system.

7.1.1.3 Maintenance, Upgrade, and Flaw Remediation Procedures

Over the lifecycle of IT products, threats evolve and flaws are discovered. To ensure continued secure operation of a system, components need to be accompanied by procedures for maintaining system security, applying upgrades and addressing flaws. The documentation describing these procedures should be clear, detailed, and sufficient to ensure that each component is maintained in the secure state established in the installation, start-up and administration guides.

System designers should evaluate these procedures to ensure that they maintain the security of the system.

The administrator should use the system maintenance procedures to carry out preventive and corrective maintenance.

The administrator should use the upgrade procedures to regularly patch the system. The administrator should ensure that all systems and applications have the proper patches and security updates applied.

The administrator should use the system flaw remediation procedures to inform the system designer and the system vendor of applicable incidents as discussed in Section 6.9.

7.1.2 Design Documents

The requirements specified in this section should be applied during the selection of the products. These documents should describe a system that meets the security functional requirements of the application in question. The system should be evaluated against these documents prior to the deployment, to ensure that the product design is sound, the delivered system meets the design requirements, and that the design process included at least the following documents:

1. Functional Specification
2. Complete External Interfaces Specification consisting of the following for each interface:
    a) Inputs
    b) Processing (high level description)
    c) Outputs
    d) Errors
    e) Exceptions and Side Effects
3. System Architecture consisting of the following:
    a) Description of Major Functional Components
    b) External IT Entities
    c) System Interfaces
    d) Application Work-flow
4. High Level Design

7.2 Vulnerability Analysis

The documentation specified in this section should be analyzed during the selection of the products to ensure that comprehensive vulnerability testing was conducted by the vendor, and that the vulnerability testing included the following documents:

1. Vulnerability analysis methodology
2. Databases searched to conduct vulnerability analysis, including queries made to the NVD
3. Vulnerability analysis finding
4. Vulnerability confirmation or refutation (e.g., based on in-depth analysis or empirical penetration testing)
5. Actions taken to close any identified vulnerabilities
6. Residual vulnerabilities and proposed mitigations for these

System designers should review this documentation to ensure that IT components deployed will meet the security requirements of the UOCAVA system.

7.3 Testing Requirements

The requirements specified in this section should be applied during the selection of the products to ensure that comprehensive security testing was conducted, and that the security testing included the following documents:

1. Test plan and degree to which the external interface specification was tested. It is required that the external interface testing was comprehensive. Testing is considered comprehensive if every external interface is tested for nominal and boundary conditions and every error for each external interface is exercised.
2. Test cases and test procedures
3. Automated test scripts
4. Test results

System designers who are making use of COTS components should review the security testing documentation which accompanies these, ensure that IT components deployed will meet the security assurance requirements of the UOCAVA system, and reference the component testing documentation when documenting the entire system.

8 References

8.1 Documents and Papers

CEMv3.1	Common Methodology for Information Technology Security Evaluation – Evaluation methodology, July 2009, Version 3.1 Revision 3 Final http://www.niap-ccevs.org/cc_docs/CEMV3.1R3.pdf
GAO08536	GAO Report 08-536, Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information, May 2008, http://www.gao.gov/new.items/d08536.pdf
HAVA	Help America Vote Act of 2002 http://www.fec.gov/hava/law_ext.txt
NISTIR-7298	Glossary of Key Information Security Terms http://csrc.nist.gov/publications/nistir/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf
NISTIR-7551	A Threat Analysis on UOCAVA Voting Systems, December 2008 http://www.nist.gov/itl/vote/upload/uocava-threatanalysis-final.pdf
OMB0404	E-Authentication Guidance for Federal agencies, OMB Memorandum M-04-04, December 16, 2003 http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
PILOTREQ	UOCAVA Pilot Program Testing Requirements, March 24, 2010 http://www.eac.gov/program-areas/voting-systems/docs/requirements-03-24-10-uocava-pilot-program
RFC2865	Remote Authentication Dial In User Service (RADIUS), June 2000 http://www.ietf.org/rfc/rfc2865.txt
RFC5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008 http://www.ietf.org/rfc/rfc5280.txt?number=5280
RUBIN	Security Considerations for Remote Electronic Voting over the Internet, Avi Rubin, AT&T Labs – Research
SERVE	A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE), Avi Rubin, et. al., 2004
SP800-122	Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), April 2010. http://csrc.nist.gov/publications/drafts/800-122/Draft-SP800-122.pdf
SP800-123	Guide to General Server Security, July 2008 http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf
SP800-191	Guideline for The Analysis Local Area Network Security, 9 November 1994 http://csrc.nist.gov/publications/fips/fips191/fips191.pdf
SP800-24	PBX Vulnerability Analysis http://csrc.nist.gov/publications/nistpubs/800-24/sp800-24pbx.pdf
SP800-41	Guidelines on Firewalls and Firewall Policy (Draft), July 2008 http://csrc.nist.gov/publications/drafts/800-41-Rev1/Draft-SP800-41rev1.pdf

SP800-44	Guidelines on Securing Public Web Servers, Version 2, September 2007 http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf
SP800-45	Guidelines on Electronic Mail Security, Version 2, February 2007 http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf
SP800-63	Electronic Authentication Guideline, Draft NIST Special Publication 800-63-1, December 8, 2008 http://csrc.nist.gov/publications/drafts/800-63-rev1/SP800-63-Rev1_Dec2008.pdf
SP800-88	Guidelines for Media Sanitization, September 2006 http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf
SP800-92	Guide to Computer Security Log Management, September 2006 *http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf*
SP800-94	Guide to Intrusion Detection and Prevention Systems (IDPS), February 2007 http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf
TCSEC	Trusted Computer System Evaluation Criteria, 1985 http://csrc.nist.gov/publications/history/dod85.pdf
UOCAVA	The Uniformed and Overseas Citizens Absentee Voting Act http://www.usdoj.gov/crt/voting/misc/activ_uoc.php
UOCAVA-BP	Best Practices for Facilitating Voting by U.S. Citizens Covered by the Uniformed and Overseas Citizens Absentee Voting Act, September 2004 http://www.dos.state.pa.us/election_reform/lib/election_reform/Best_Practices_for_Facilitating_Voting_by_US_Citizens_Covered_by_the_UOCAVA_EAC.pdf

8.2 Useful Websites

Federal Voting Assistance Program	http://www.fvap.gov/
How E-voting Works, Kevin Bonsor and Jonathan Strickland:	http://people.howstuffworks.com/e-voting.htm
US Election Assistance Program, Resources for Overseas Citizens and Military Voters:	http://www.eac.gov/voter/overseas-citizens-and-military-voters
National Checklist Program (NCP)	http://checklists.nist.gov/
National Vulnerability Database (NVD)	http://nvd.nist.gov/
Security Content Automation Protocol (SCAP) specifications	http://scap.nist.gov/

9 List of Acronyms

ABAC	Attribute Based Access Control
ACE	Access Control Entry
ACL	Access Control List
AES	Advanced Encryption Standard (a symmetric key based data encryption algorithm)
AH	Authentication Header
ASP	Active Server Pages
CA	Certification Authority
CAVP	Cryptographic Algorithm Validation Program
CBAC	Capability Based Access Control
CBC	Cipher Block Chaining
CCM	Counter with CBC Message Authentication Code
CD	Compact Disc
CGI	Common Gateway Interface
CMAC	Cipher-based Message Authentication Code
COTS	Commercial-Off-The-Shelf
CRL	Certificate Revocation List
CSRF	Cross Site Request Forgery
DAC	Discretionary Access Control
DDoS	Distributed Denial of Service
DH	Diffie Hellman
DMZ	Demilitarized Zone
DNS	Domain Name Service
DoS	Denial of Service
DVD	Digital Video Disc
EAC	Election Assistance Commission
FTP	File Transfer Protocol
HAVA	Help America Vote Act
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
I&A	Identification and Authentication
ICMP	Internet Control Message Protocol
ID	Identifier
IDS	Intrusion Detection System
IE	Internet Explorer (Microsoft web browser application software)
IETF	Internet Engineering Task Force

IMAP	Interactive Mail Access Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IT	Information Technology
KBA	Knowledge Based Authentication
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Mandatory Access Control
MAC	Message Authentication Code
MITM	Man-In-The-Middle
NBA	Network Behavior Analysis
NCP	National Checklist Program
NetBIOS	Network Basic Input/Output System
NFS	Network File System
NIS	Network Information System
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
NVD	National Vulnerability Database
OCSP	Online Certificate Status Protocol
OTP	One Time Password
PBAC	Privilege Based Access Control
PBX	Private Branch Exchange
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POP	Post Office Protocol
RADIUS	Remote Authentication Dial In User Service
RAID	Redundant Array of Inexpensive Disks
RBAC	Role Based Access Control
RDBMS	Relational Data Base Management System
RFC	Request For Comment (series of standards developed by IETF)
RSA	Rivest, Shamir, Adelman (a public key cryptography algorithm)
SAN	Storage Area Network
SASL	Simple Authentication and Security Layer
SCAP	Security Content Automation Protocol
SHA-1	Secure Hash Algorithm (Version 1) – a FIPS Standard
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol

SP	Special Publication (A National Institute of Standards and Technology publication series)
SQL	Structured Query Language
SSH	Secure Shell
SSI	Server Side Include
SSL	Secure Socket Layer
SSN	Social Security Number
TCP	Transmission Control Protocol
TDES	Triple Data Encryption Standard (a symmetric key based data encryption algorithm)
TLS	Transport Layer Security
UDP	User Datagram Protocol
UOCAVA	Uniformed Overseas Citizens Absentee Voting Act
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WORM	Write-Once Read Many
XSS	Cross-Site Scripting

10 Glossary

Access Control	The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services
Access Control Entry (ACE)	An entity and the type of permission granted to that entity, contained on an Access Control List
Access Control List	A register of: 1. users (including groups, machines, processes) who have been given permission to use a particular system resource, and 2. the types of access they have been permitted.
Certificate	A digital representation of information which at least 1. identifies the certification authority issuing it, 2. names or identifies its subscriber, 3. contains the subscriber's public key, 4. identifies its operational period, and 5. is digitally signed by the certification authority issuing it.
Certificate Revocation List (CRL)	A list of revoked public key certificates created and digitally signed by a Certification Authority.
Certification Authority (CA)	A trusted entity that issues and revokes public key certificates
Commercial-Off-The-Shelf (COTS)	Hardware and software IT products that are ready-made and available for purchase by the general public
Cross-Site Request Forgery (CSRF)	A type of web exploit where an unauthorized party causes commands to be transmitted by a trusted user of a website without that user's knowledge
Demilitarized Zone (DMZ)	A network created by connecting two firewalls. Systems that are externally accessible but need some protections are usually located on DMZ networks
Denial of Service (DoS)	The prevention of authorized access to resources or the delaying of time-critical operations.
Discretionary Access Control (DAC)	The basis of this kind of security is that an individual user, or program operating on the user's behalf is allowed to specify explicitly the types of access other users (or programs executing on their behalf) may have to information under the user's control.
Distributed Denial of Service (DDoS)	A Denial of Service technique that uses numerous hosts to perform the attack
Hash-based Message Authentication Code (HMAC)	A message authentication code that uses a cryptographic key in conjunction with a hash function.
Identification and Authentication (I&A)	The process of establishing the identity of an entity interacting with a system
Intrusion Detection System (IDS)	Software that looks for suspicious activity and alerts administrators.
Intrusion Prevention System (IPS)	System which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.
Man-In-The-Middle (MITM)	An attack where the adversary positions himself in between the user and the system so that he can intercept and alter data traveling between them.
Mandatory Access Control (MAC)	Access controls (which) are driven by the results of a comparison between the user's trust level or clearance and the sensitivity designation of the information.

Message Authentication Code	A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data.
Metacharacter	A character that has some special meaning to a computer program and therefore will not be interpreted properly as part of a literal string.
Network Behavior Analysis	Examination of network traffic to identify threats, usually as part of an IDS or IPS.
Nonce	A value used in security protocols that is never repeated with the same key. For example, challenges used in challenge-response authentication protocols generally must not be repeated until authentication keys are changed, or there is a possibility of a replay attack. Using a nonce as a challenge is a different requirement than a random challenge, because a nonce is not necessarily unpredictable.
Out Of Band	Used to refer to information transmitted through a separate communications channel.
Personally Identifiable Information (PII)	This is information which can be used, alone or in combination with other information, to distinguish or trace an individual's identity.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Token	Something a user possess and controls used to authenticate the user's identity.
Transport Layer Security (TLS)	An authentication and encryption protocol widely implemented in browsers and web servers. HTTP traffic transmitted using TLS is known as HTTPS.
UOCAVA	Uniformed Overseas Citizens Absentee Voting Act
UOCAVA Systems	Information technology systems which enable uniformed and overseas United States citizens to vote.
XSS	Cross-Site Scripting (XSS) is a security flaw found in some web applications that enables unauthorized parties to cause client-side scripts to be executed by other users of the web application