

# OKALOOSA DISTANCE BALLOTING PILOT



## **Procedures and System Description for Secure Remote Electronic Transmission of Ballots for Overseas Civilian and Military Voters**

Reference: Florida Administrative Rule 1S-2.030  
Electronic Transmission of Absentee Ballots

**June 19, 2008**

# TABLE OF CONTENTS

Section 1. Introduction.....	3
Section 2. Project Overview.....	4
Section 3. Timetable and Process for Notifying Voters.....	6
Section 4. Instructions for Voters.....	7
Section 5. Election Timetable.....	8
Section 6. Remote Electronic Access Voting System Description.....	9
Section 7. Remote Electronic Access Voting System Set Up.....	11
7.1 Voter Authentication System.....	11
7.2 Remote Access Voting System.....	11
7.2.1 Secure Voting Server.....	11
7.2.2 Kiosk Voting Stations.....	11
7.3 Kiosk Sites.....	12
7.4 Creation of Election Cryptographic Keys.....	12
Section 8. Remote Access Voting Process.....	14
8.1 Voter Identification and Authentication: Standard Processing.....	14
8.2 Voter Identification and Authentication: Exception Processing.....	14
8.3 Activating the Ballot and Voter Digital Certificate.....	15
8.4 Voter Verification of Paper Record and Casting of Ballot.....	15
Section 9. Absentee Ballot Canvassing and Tabulation.....	17
9.1 Ballot Canvassing.....	17
9.2 Ballot Decryption and Tabulation.....	18
9.3 Creating an Integrated Tabulation Report.....	18
Section 10. Election Closeout.....	19
10.1 Closing Kiosk Locations.....	19
10.2 Consolidation and Archiving of Election Materials.....	19
10.3 Voter Confirmation of Ballot Receipt.....	19
Section 11. Remote Electronic Access Voting System Security.....	20
11.1 Kiosk Sites.....	20
11.1.1 Ballot Casting Process.....	20
11.1.2 Voter Authentication.....	22
11.2 Data Centers.....	22
11.2.1 Voting System.....	22
11.2.2 Voter Authentication.....	25
11.3 Okaloosa County Elections Office.....	25
11.4 Communications.....	27

## **SECTION 1 INTRODUCTION**

This document has been prepared pursuant to Florida Administrative Rule 1S-2.030 Electronic Transmission of Absentee Ballots. This rule permits a supervisor of elections to provide the option of voting by secure remote electronic transmission for overseas absentee voters if certain requirements are met. One of these requirements is the submission of a written plan for approval by the State Division of Elections. The plan must be submitted no later than four (4) months prior to the intended use of this voting option in an election. The plan must contain, as a minimum, all the information specified in Section 8 of the rule.

The Supervisor of Elections of Okaloosa County proposes to conduct a pilot project using secure remote electronic transmission for the November 2008 general election. For ease of reference, this project is entitled the Okaloosa Distance Balloting Pilot (ODBP). This document is the plan required for that intended use. Specific provisions of the administrative rule are referenced where the text is directly responsive to the rule. Additional information is included to provide a complete description of the election administration processes and the proposed system.

## **SECTION 2 PROJECT OVERVIEW**

Okaloosa County, Florida, is the home of Eglin Air Force Base, Hurlburt Field, Duke Field, U.S. Army Ranger Camp Rudder, the Navy EOD School, and a Coast Guard station. It is “home” to a great many active duty members and their dependents here and around the world. Over 20,000 of them are registered voters in Okaloosa County. Since the late 1990s the drawdown in overall troop strength combined with increased requirements for U.S. military presence abroad have raised the mobility demands for both active duty and reserve units. In addition, ever larger numbers of civilian contractors are also deployed to support the heightened pace of operations. Today’s constant critical deployment schedules provide pressing motivation to improve the overseas absentee voting process.

The county elections office has participated in numerous projects exploring alternative solutions, but has been frustrated by the fact that none has moved beyond the experimental phase. Consequently, the Supervisor of Elections has decided to conduct her own pilot project with the express intention of developing a solution that subsequently can be implemented as a standard election administration process in the county. This solution could potentially also provide a model for other counties with large overseas military and/or civilian voter populations.

The Okaloosa Distance Balloting Pilot (ODBP) project will establish a secure and scalable distance balloting environment for approximately 600 self-selecting overseas voters. This environment will be created by placing supervised absentee voting kiosks in three overseas locations. Each kiosk location will be staffed by election officials. The kiosk voting stations will employ proven, transparent, and secure electronic remote voting technology and will be operated under the management and control of the Supervisor of Elections. The voting stations are connected to a secure voting server in Florida by a secure Virtual Private Network (VPN). The overseas locations will be selected for their proximity to Okaloosa voters based at U.S. military installations in Mildenhall, England; Ramstein, Germany; and Kadena, Japan. The kiosks will be available for ten days (October 24<sup>th</sup> through November 2<sup>nd</sup>) prior to the election and open to all qualified military and civilian voters in the vicinity who have submitted a request to vote by this method.

As citizens present themselves to vote, the election officials will validate each person’s identity, verify their eligibility to vote, and determine their ballot style, using a laptop with on-line access to the Florida statewide voter registration database. Each voter will be assigned a unique digital certificate to sign their voted ballot. The voter will use a secure voting station to connect to a secure voting server to view the ballot, make ballot selections, and confirm their choices using a summary screen. A paper record of the voter’s ballot selections will be printed for the voter’s review and securely stored for audit or recount use.

When the voter casts his or her ballot, it is electronically enclosed in a digital envelope and encrypted using the Okaloosa election public key. It is then signed with the voter’s

digital certificate to further protect the integrity of the ballot and guarantee its authenticity. The secured ballot is transmitted via VPN to the secure server where it is stored until the time for ballot canvassing. Each voter will receive a “counted as cast” receipt that allows them to individually verify that their vote was included in the final election tabulation. This receipt does not contain any indication of how the voter voted so it cannot be used for vote selling or other fraudulent purposes.

At the close of polls, the Okaloosa Canvassing Board will meet to collectively reconstruct the election private key to decrypt the ballots. The order of the ballots is mixed during the decryption process to prevent any correlation between ballots and voters. The Canvassing Board will tabulate the ballots and prepare a combined tabulation report for all the kiosk locations. This report will be incorporated manually into the final election tabulation report. The mixing process also generates a list of “counted as cast” receipt codes. This list will be posted on the Okaloosa County Supervisor of Elections website so voters can verify that their ballots were counted.

### **SECTION 3      TIMETABLE AND PROCESS FOR NOTIFYING VOTERS**

**[Reference rule (2)(d)4,(8)(a)1]**

In March 2008, voters in the regions around the kiosk site areas in Germany, the UK, and Japan were notified by a letter detailing the following:

- An explanation of the program.
- A solicitation of name of local Voting Assistance Officer (VAO) (if known).
- An explanation of any restrictions.
- A solicitation of the voter's e-mail address.
- Information about the availability of the application form required to be submitted by the voter to request receiving his or her ballot by this means.

The e-mail addresses will populate a contact list to enable the Supervisor of Elections (SOE) to keep interested voters engaged and informed about the project's progress. Getting the names of local VAOs will enable direct contact with them about the project, which may help reach additional eligible participants.

Along with pilot project information, the required application form will be made available on the Okaloosa County SOE website, soliciting the information normally required to identify voters, such as:

- Overseas mailing address
- Residence address
- Date of birth
- E-mail address

## **SECTION 4      INSTRUCTIONS FOR VOTERS**

**[Reference rule (8)(a)2]**

Voters who have pre-elected to participate in ODBP will receive two specific sets of instructions to inform them how to participate at one of the kiosk sites. The first instruction set will be emailed to participants at least one month before the voting period begins and will provide detailed information regarding kiosk location and what they must bring with them in order to vote. At a minimum, these instructions will contain the following information:

- Information about participation.
- A notice of the requirement to bring appropriate identification.
- The time period of operation, hours available, and locations of the kiosk sites.
- An explanation of the voter's responsibilities regarding the Voter's Choice paper record.
- A pointer to the Okaloosa SOE website that provides detailed information about the ODBP voting process, a sample ballot, and other election information

The second set of instructions will be provided to each participant at the kiosk site. These instructions will detail the voting procedure. Each kiosk will also have posters and leaflets explaining in a simple and graphical way how to use the voting stations.

**SECTION 5 ELECTION TIMETABLE**  
**[Reference rule (8)(a)3]**

**Table 1**

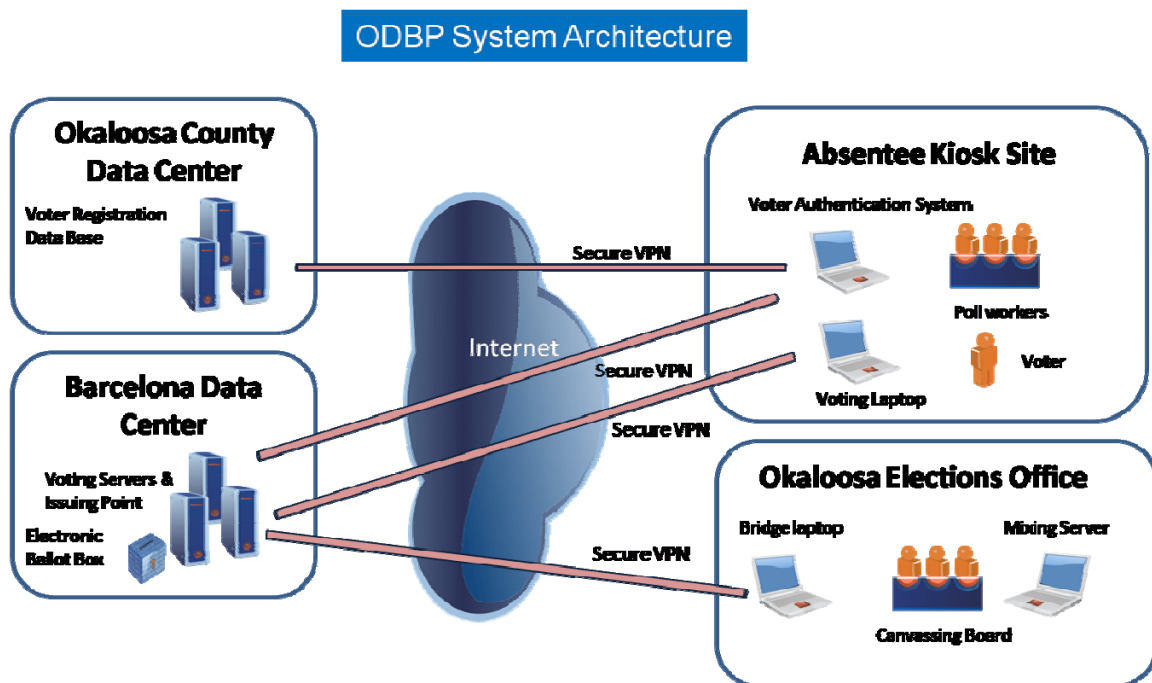
<b>Date</b>	<b>Activity</b>
7 Mar 2008	Information letter sent to voters in regional kiosk areas
27 May 2008	Kiosk Election Officials selected
June 2008	Orientation of selected Kiosk Election Officials
Ongoing	Monthly updates to voters and project participants
Aug (est.) 2008	Certification of ODBP system under FL VSS
Aug 2008	Kiosk site locations finalized
Sep 2008	Training of Kiosk Election Officials and Alternates
1-10 Oct 2008	Configuration of the election in the voting platform
13-16 Oct 2008	Staging, final checks of equipment, software, supplies
18-19 Oct 2008	Travel to kiosk sites for Kiosk Election Officials
20-22 Oct 2008	Setup, final testing, and preparation of kiosk equipment
24 Oct 2008	Kiosk voting begins <i>See TABLE 2 below for disposition of types of election data</i>
2 Nov 2008	Kiosk voting ends
2 Nov 2008	Kiosk sites shut down, equipment, software, other materials prepared for return
3 Nov 2008	Return travel day for Kiosk Election Officials
3 Nov 2008	Canvass of electronic ballots completed by Canvassing Board
4 Nov 2008	After 7 PM—decrypt and tabulate electronic ballots
4 Nov 2008	All kiosk equipment, software, voter certificates and other paperwork secured in SOE vault
5 Nov 2008	“Counted As Cast” receipt page posted to SOE website
17 Nov 2008	Audit of ODBP system begins

**Table 2**

<b>Item</b>	<b>Disposition</b>
Voted Ballots	Encrypted and stored on the secure server at Data Center
Voter Certificates	Scanned daily and copied to folder on Okaloosa file server
Voter Choice Records	Secured in numbered, sealed transport case by the voter
Counted As Cast Receipts	Retained by voter for vote count verification

## SECTION 6 REMOTE ELECTRONIC ACCESS VOTING SYSTEM DESCRIPTION

The Remote Electronic Access Voting System will be based on Pnyx, a unique solution developed by SCYTL based on its twelve years of research experience in the electronic voting security field. The solution implements a unique and patented cryptographic protocol that, combined with physical and logical security measures, provides electronic voting platforms with the highest security levels available today. For the ODBP project the Remote Electronic Access Voting System will be deployed as displayed in the figure below:



The Pnyx platform is comprised of four main components:

- 1) The Voting Client: a computer program (e.g., a Java applet running on a standard web browser) that authenticates the voter, displays the correct ballot style to the voter, and encrypts the ballot following a special cryptographic protocol. In the ODBP project the Voting Client will be a Java application executed in the Voting Laptop (running on a Live CD) at each remote kiosk site.
- 2) The secure Voting Servers: the servers that execute the server side of the cryptographic protocol, store the encrypted ballots in an electronic ballot box, and verify the electronic identity of the voters. In the ODBP project the Voting Server(s) will be hosted in a secure data center in Barcelona, Spain. Each Voting Laptop will connect to the Voting Server through a secure VPN. No other connections will be allowed.
- 3) The Bridge Laptop: a laptop that is used to download the encrypted electronic ballot box from the voting servers using a VPN connection.

4) The Mixing Server: a server that is used to create the election cryptographic keys before the election is opened, and to decrypt the ballots and execute the Mixing protocol at the end of the election. In the ODBP project, this server will be isolated from any network (air gapping), and will be securely stored inside the vault managed by the Okaloosa Elections Office staff. The data that this server will process will be transferred by removable physical storage media (e.g., USB memory pen) from/to the Bridge Laptop.

The ODBP project requires a Voter Authentication System which is used to verify the voter's eligibility to vote, print the Voter's Certificate, and write the voter ID, PIN code, precinct ID, and ballot style data to the smartcard used to activate the ballot at the Voting Laptop. The current Okaloosa VRDB and associated applications provide the voter eligibility checking and the printing of the Voter's Certificate. The generation of the data for the smartcard will be a new application written for this purpose.

The main features offered by Pnyx are as follows:

- End-to-end security (from the voter to the Canvassing Board) by putting the control of the electoral process in the hands of the Supervisor of Elections rather than a system administrator.
- Integrity of election results by preventing the addition of bogus votes and the manipulation or elimination of valid votes.
- Strong authentication of each voter's ballot by using unique digital signatures.
- Voter privacy by sealing votes in digital envelopes and implementing a Mixing protocol to break the correlation between votes and individual voters.
- Election auditability by providing election authorities and third parties with means to fully audit the electoral process.
- Voter-verifiability by providing voters with counted as cast receipts that, without disclosing the voter's choices, allow them to individually check that their votes have reached the Canvassing Board and have been counted.
- Secrecy of intermediate results by protecting the integrity of the electronic ballot box.
- Usability by providing an accessible and user-friendly voter interface.
- Multi-channel elections since it can be easily integrated with other voting channels.
- Scalability by being based on a flexible platform with significant economies of scale.
- Availability as it can be deployed in redundant configurations.
- Accuracy since it prevents voters from making unintentional selection mistakes that could invalidate their votes (e.g., over-voting or under-voting).

## **SECTION 7     REMOTE ELECTRONIC ACCESS VOTING SYSTEM SET UP**

### **7.1 Voter Authentication System**

Voter authentication will be provided by a hardened laptop containing the Okaloosa voter registration database and an application which allows the kiosk officials to verify a voter's eligibility to vote and to update voter history. This laptop is connected by VPN to the voter registration system in Okaloosa County so that all voter registration data is kept in sync. A standard printer will be connected to the laptop to print Voter Certificates. A bar code scanner will be connected to the laptop to read the bar codes on the printed Voter Certificates. This data is used to record the Voter Credentials (voter ID and PIN code) and ballot style indicator on a smartcard. This card will be inserted into the voting station to activate the ballot as described below.

There will be two Voter Authentication Systems at each kiosk site: one for use, and the other as back-up.

### **7.2 Remote Access Voting System**

#### ***7.2.1 Secure Voting Server***

As part of system set-up, Okaloosa election staff will create a CVS file from the Voter Registration Database containing the following data: voter first and last names, voter registration number, precinct, and ballot style. This information will be used to generate digital certificates and PIN codes for each of these voters. The digital certificates will be stored on the secure voting server.

The Okaloosa election staff will export/extract the ballot definition data from the GEMS tabulation server. This file will be loaded into the voting application which will present the appropriate ballot style when a smartcard is inserted into the Voting Laptop.

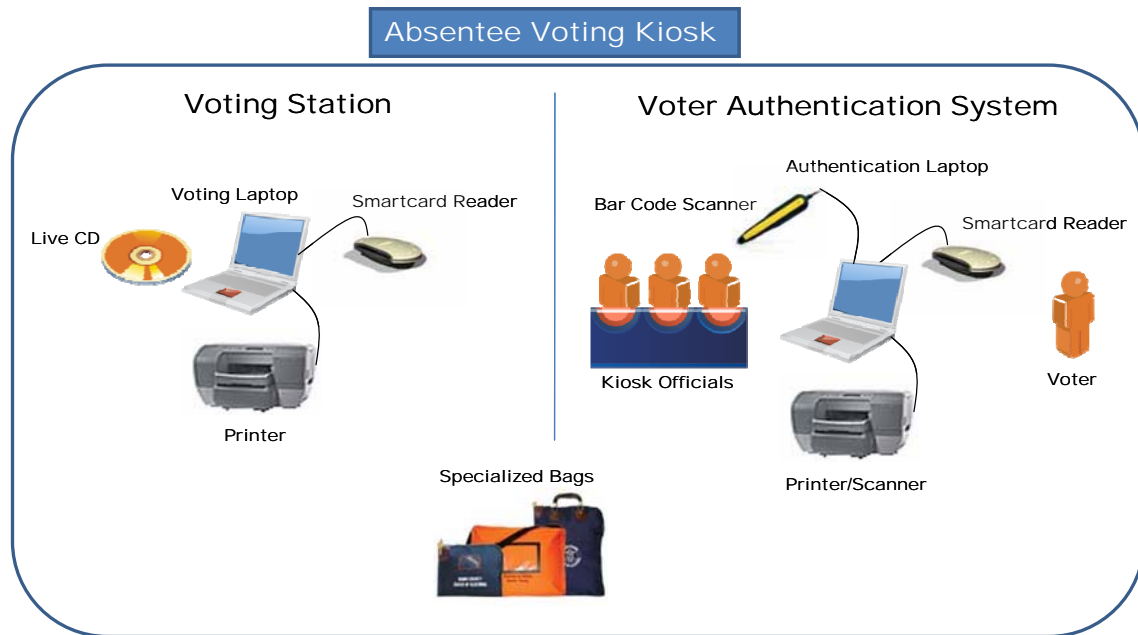
#### ***7.2.2 Kiosk Voting Stations***

The kiosk Voting Stations will be composed of a laptop (with no hard disk), a printer, smartcard reader and a Live CD that contains the voting software. The laptop will be connected through a VPN to the secure Voting Server. The smartcard reader attached to the laptop will be used to electronically activate the correct ballot style and voter digital certificate using the data stored in the smartcard provided to the voter by the Voter Authentication System. There will be two fully-equipped Voting Stations per kiosk site: one for voting, and the other for back-up.

### 7.3 Kiosk Sites

[Reference rule (8)(a)6]

The setup of all kiosk hardware and initialization of software will be accomplished by the kiosk Election Officials, with technical support from Scytl, if required. All equipment and software will be checked out in the SOE office before being transported to the kiosk sites. Chain of custody control will be required for the laptops and software CDs. The system configuration at all sites will resemble the following diagram:



### 7.4 Creation of Election Cryptographic Keys

[Reference rule (8)(b)1.a.,b.]

Before voting begins at the kiosk locations, the Okaloosa Canvassing Board will meet to create the cryptographic keys that will be used to encrypt and decrypt the ballots. This will be done in the Mixing Server, located in the SOE office. This same server will also be used at the end of the election to decrypt the ballots. SOE staff will operate the system to generate a unique pair of asymmetric cryptographic keys, consisting of a public key and a private key. The public key will be used to encrypt the ballots cast by the voters at the kiosk Voting Stations by means of a digital envelope. The private key will be used at the end of the election to decrypt the ballots (i.e., opening of the digital envelope).

Before voting begins at the kiosk locations, the private key will be divided into segments called "shares" which will be distributed among the members of the Canvassing Board. Each member of the board will type a private password twice into the key generating application, and he or she will receive a smartcard containing a protected share. When the shares have been distributed, the private key will be securely erased from the system. Therefore, during the voting period, the contents of the cast ballots cannot be viewed by anyone since they are encrypted and the private key to decrypt them can only be

generated by the collaboration of a previously determined number of Canvassing Board shares. At the end of the voting period the members of the Canvassing Board will meet to reconstruct the private key (by contributing their shares) and decrypt the ballots in the Mixing Server.

After the process to create the election cryptographic keys is completed, the Mixing Server will be stored in the secure vault managed by the Okaloosa elections office staff. It will be used again at the end of the election to decrypt and canvass the electronic ballots.

## **SECTION 8      REMOTE ACCESS VOTING PROCESS**

**[Reference rule (8)(a)4,5,(8)(b)4,5,6,7]**

### **8.1 Voter Identification and Authentication: Standard Processing**

*[Reference rule (8)(b)4]*

The first steps in the voting process are to authenticate the voter's identity and verify his or her eligibility to vote. The following workflow is for the standard process. This is the case where the voter has an appropriate form of identification (ID), their name and current address are in the voter registration database, and they are eligible to vote.

- The voter arrives at a kiosk location and presents a photo ID. Kiosk operating procedures will include a list of types of IDs that are acceptable for this purpose.
- The kiosk official looks up the voter in the voter registration database (VRDB) to verify their eligibility to vote. When his or her name is found, the voter is asked to provide their voting address to compare with the address in the database.
- If the addresses match a Voter Certificate is printed. This contains the election identifier, precinct number, ballot style, voter's name, address, date of birth, voter registration number, and a barcode of the voter registration number. The Certificate also includes the state oath, which the voter signs.
- The bar code on the Voter Certificate is scanned in order to write on a smartcard the Voter Credentials (Voter ID and PIN code) and the corresponding ballot style. The smartcard will be used to activate the ballot on the Voting Laptop.
- The signed Voter Certificate will be scanned to a PDF file and stored locally on the Voter Authentication Laptop hard drive. The file name will be Voter ID-yyyyymmdd (year, month,day). Once a day these files will be uploaded through the VPN to a shared folder in the Okaloosa voter registration server so that copies of all Voter Certificates will be available for reference when needed by the Canvassing Board to canvass absentee ballots. The original documents will be securely stored at the kiosk locations and transported to Okaloosa County when the kiosk locations are closed.

### **8.2 Voter Identification and Authentication: Exception Processing**

- If the voter's residence or mailing address has changed, the kiosk official can update this information in the voter registration database (VRDB) using an application on the Voter Authentication laptop. If this change does not affect the voter's ballot style, the standard process will be followed.
- If a change in residence address requires the assignment of a different ballot style, the kiosk official can determine the appropriate ballot style through a geographic lookup application that is part of the VRDB system, and update the database with this information. Then the standard process is followed.
- The voter must submit any other changes, such as name or political party affiliation, in writing to the Supervisor of Elections.

### **8.3 Activating the Ballot and Voter Digital Certificate**

*[Reference rule (8)(a)4]*

- The voter is escorted with the smartcard containing their Voter Credentials and ballot style to the Voting Laptop and, in view of the kiosk election official, inserts the smartcard in the available reader. Then the voter presses a button on the screen to continue.
- The voting application will read the contents of the smartcard. The ballot style and Voter ID are communicated to the Voting Server which stores the ballot style definitions, the ballot data, and the digital certificates associated with each voter. The server will generate and transmit the appropriate ballot style for display on the Voting Laptop, along with the voter's digital certificate and associated keys.
- The PIN code is used to 'unblock' the voter's digital certificate and associated keys in the laptop. The PIN code is not sent to the secure server but is retained by the Voting Laptop. Once unblocked, the voter's keys are used to encrypt the ballot when it is cast. This process is transparent to the voter.
- The voter makes his or her ballot selections. The system will not allow over-votes and will supply a notice to the voter of any under-votes. When the voter has completed voting, the system presents a summary screen so the voter can confirm his/her choices. The ballot summary is also sent to the printer attached to the laptop.

### **8.4 Voter Verification of Paper Record and Casting of Ballot**

*[Reference rule (8)(a)5]*

- When the voter reaches the summary screen, the system will automatically print the ballot summary as a paper record on a printer attached to the Voting Laptop. This paper record will also contain a unique random number.
- The voter will review the paper record and then press the vote button to cast the ballot. When the button is pressed, the voting application encrypts and digitally signs the voted ballot using the voter's digital certificate. The ballot is immediately transmitted back to the Voting Server where it is stored until the absentee ballot canvassing process occurs.
- If the voter opts to change one or more of his choices, a new paper record will print. Each new paper record will include a 'version identifier' with the unique random number (e.g., 10001A, 10001B, etc. where "A", "B" are the version identifiers). All versions of the paper record, up to a maximum of three, will be deposited in a secure receptacle to be retained as part of the election record. In the event of a recount or audit, only the last one of multiple paper records will be used since it corresponds to the cast electronic vote.
- The voter will also receive a "counted-as-cast" receipt that can be used after the election to confirm that their ballot was received and counted by the Canvassing Board. These receipts do not contain any information as to how the voter voted, but only a unique code for that voter. This code is randomly generated by the voting station, and included inside the encrypted ballot. After the ballots are decrypted, only the Canvassing Board can access these codes and publish them to the webpage where

- The voter completes the voting process by depositing the paper record(s) in a secure receptacle adjacent to the Voting Laptop. The voter will also return the smartcard to the kiosk officials, so it can be re-used with the following voters.

## **SECTION 9      ABSENTEE BALLOT CANVASSING AND TABULATION**

**[Reference rule (8)(b)6,7]**

### **9.1 Ballot Canvassing**

On November 3, the Canvassing Board will check the ‘facial validity’ of the electronic ballots stored on the Voting Servers. In addition to having the Voter Certificates with voters signatures, the Board can also use the voter ID number to retrieve data from the Voting Servers, such as date and time ballot was cast, , location of kiosk, and ballot style.

Following standard canvassing procedures, the Canvassing Board will review each voter’s eligibility and signature and determine whether to designate ballots as ‘valid’ or ‘rejected’. A reason must be recorded for each rejected ballot. Possible reasons are the voter is not eligible to vote or the signature on the Voter’s Certificate doesn’t match the signature in the VRDB.

The kiosk ballot canvassing must be coordinated with the by-mail ballot canvassing to ensure that no more than one ballot is counted for each voter. During the UOCAVA absentee voting period, the Okaloosa elections staff will maintain a list of all by-mail ballots received from voters located in the vicinity of the voting kiosks. These ballots will be put aside for processing after the kiosk locations have closed. At this time it can be determined whether a voter has also voted an electronic ballot. In the event both paper and electronic ballots are received, the electronic ballot will be counted and the paper ballot set aside as a duplicate. Should a paper ballot inadvertently be processed and placed in the ballot box prior to kiosk canvassing, this ballot is required to be counted instead of the electronic one.

When all the ballots have been reviewed, a copy of the electronic ballot box will be downloaded from the Voting Servers to the Bridge Laptop by a member of the Administration Board under the supervision of the Canvassing Board. The downloaded ballots will be tagged as ‘valid’ or ‘rejected’. This file will then be copied to removable media (e.g., CD-ROM or USB memory stick) and installed on the Mixing Server in preparation for decryption and tabulation.

To protect the integrity of the electronic ballot box, verifying ballot validity can only be performed using the ballot reconciliation application that runs on the Voting Servers. It cannot be performed on the downloaded electronic ballot box. However, the electronic ballot records are retained on the Voting Servers until election closeout. (See Section 10.) Therefore, ballot canvassing could be performed more than once, if needed. This will also allow auditing the performance of this function for project evaluation purposes after the election.

## **9.2 Ballot Decryption and Tabulation**

When the electronic ballot box is loaded on the Mixing Server, the Canvassing Board will reconstruct the election private key and process the accepted ballots. The decryption and tabulation process is initiated by each of the Board members inserting their smart card with a key share into the Mixing Server and entering their personal password . Once the election private key is reconstructed, the system will execute a mixing process that breaks the correlation between voters and ballots and decrypts the ballots. The end result is a list of ‘clear votes’ and a list of the counted as cast receipt codes. The votes are then tallied by the system and a tabulation report produced in PDF that provides all the required tabulation data, (e.g., undervotes, blank votes, write-in votes).

## **9.3 Creating an Integrated Tabulation Report**

The tabulation report from the Scytl Pnyx system will be manually uploaded to the GEMS system by Okaloosa election staff, creating an air gap between the ODBP system and the tabulation system.

## **SECTION 10 ELECTION CLOSEOUT**

### **10.1 Closing Kiosk Locations**

Once the remote voting process is closed, the kiosk officials can decommission the components of each kiosk site. As all the electronic ballots were stored in a secure voting server and the VRDB was updated in real time, only the paper records and Voter Certificates need to be stored in secure receptacles.

As part of the decommissioning, all equipment associated with the voting station and the voter registration system will be packed to be sent back to Okaloosa. The CDs containing the voting station software will be removed and securely stored for transport by the kiosk officials to Okaloosa.

### **10.2 Consolidation and Archiving of Election Materials**

The Voter Certificates, paper records, software, and other election materials from all the kiosk locations will be assembled, logged, and archived by the Okaloosa elections office staff. The electronic ballots stored in the secure server (both valid and invalid) will be stored on back-up media and archived. All the logs generated by the voting system will be copied to back-up media and archived for the required 22 months.

### **10.3 Voter Confirmation of Ballot Receipt**

*[Reference rule (8)(b)5]*

After tabulation has occurred, the system will generate a report of the counted as cast receipt codes for all ballots included in the tabulation. This report will be posted on the Okaloosa Supervisor of Elections website, so voters can confirm that their ballots were received and counted.

## **SECTION 11 REMOTE ELECTRONIC ACCESS VOTING SYSTEM SECURITY**

**[Reference rule (8)(a)5,6; (8)(b)1.a.,b.,c.;(8)(b)2.,3.,7.]**

Security is paramount in remote electronic voting, even when votes are cast from a supervised environment as in the ODBP project. The risks of using communications channels and the presence of new actors with privileges in the system (e.g., system and infrastructure administrators) must be adequately managed to prevent any security issue during the election process.

The security controls implemented in the ODBP system have been defined following an ISO 27001 risk management approach using Florida Administrative Rule 1S-2.030 as the starting point for the security requirements. After identifying the different vulnerabilities and threats to which the system is exposed, a set of security controls has been defined to prevent the materialization of these threats or to mitigate their impact.

These security controls include physical, logical, and procedural measures that will be implemented during the election process. The ODBP voting system is structured and deployed in four environments: the kiosk sites, the data centers, the Okaloosa County elections office, and the communications channel. The following sections summarize the main security measures and controls implemented in each of the four environments.

### **11.1 Kiosk Sites**

Kiosk sites will be managed by election officials who will be responsible for enabling a trustworthy and accurate voting process. It is of paramount importance to provide election officials with means to audit and verify the correct implementation of the voting process in these kiosk sites. Election officials must be able to check the integrity of the voting infrastructure and materials used by voters and themselves in order to detect any manipulation attempts. At the same time, voters must be reassured that their voting intent is correctly recorded and protected. As a result, as explained below, appropriate security measures must be used in the processes implemented at the kiosk sites: Ballot Casting and Voter Authentication.

#### **11.1.1 Ballot Casting Process**

Ballot casting takes place in the Voting Laptops. Therefore, the Voting Laptops must be adequately audited, certified and secured in order to guarantee that they behave as expected – that voter choices are recorded as intended while preserving voter privacy and the secrecy and accuracy of the vote. Any attempt to modify the Voting Laptops must be detected and reported. In addition, adequate measures must be implemented to guarantee the availability of the voting process at the kiosk sites. To achieve these objectives, the following measures are adopted.

### ***Physical measures***

- Access control to Voting Laptops: Voting Laptops will be located so that access can be controlled by the kiosk election officials.
- Tamper evident controls of Voting Laptops: Voting laptops, peripherals and connections will be protected by tamper evident seals or locks that will allow detecting any internal or external manipulation attempts.
- Use of read only media: Distribution of the voting software using bootable read-only media (Live CD-ROM). Booting from CD-ROM media reduces the risk of tampering with the software and prevents the execution of malicious software. The accuracy of the CD-ROM contents must be checked before booting from it.
- Secure configuration of Voting Laptops: Voting Laptops will have only the indispensable components required for the voting process. Hard disks, connection ports and peripherals not required for the process will be eliminated or disabled.
- Wired network connections: Wireless connections will be eliminated or disabled.
- Redundant equipment and spare parts: There will be redundant voting laptops and spare components.
- Tamper evident controls: The secure receptacle for the paper records will be protected by tamper evident seals or locks that will allow detection of any internal or external manipulation attempts.

### ***Logical measures***

- Remote strong authentication of voters: Each voter will be assigned a unique digital certificate through the credentials generated by the kiosk election officials. This digital certificate will be used to electronically authenticate the voter through the voting server.
- Voter privacy: The ballots are encrypted (digital envelope) in the Voting Laptops using the election public key. Only the members of the Okaloosa Canvassing Board will be able to decrypt the ballots at the end of the election by reconstructing the election private key.
- Vote secrecy: The encryption of the ballot, by using a digital envelope, also preserves the secrecy of vote.
- Vote accuracy: The encrypted ballots are digitally signed using the voter's digital certificate. This control prevents any manipulation of ballot content once it has been cast.
- End-to-end security: Cryptographic operations used to protect voter privacy and vote accuracy are implemented in the Voting Laptop before the vote is cast. Therefore, there is no risk of vote manipulation on the voting server.
- Prevention of multiple casting of votes: Voters will not be able to access more than one Voting Laptop or cast multiple ballots.
- Voter choice verification: Voters will be provided with a paper record of their ballot selections. After the verification of this record by the voter, the ballot is cast. Voters are required to deposit this paper record in a secure receptacle before leaving the kiosk site.
- Vote counted verification: Voters are provided with a counted as cast receipt after casting their ballots. The code printed on this receipt allows each voter to individually verify that his or her ballot was decrypted and counted by the Canvassing Board.

- Prevention of coercion and vote buying: Counted as cast receipt codes will not allow third parties to discern the voter's selections.

### ***Procedural measures***

- Certification of the voting software: The voting software and system configuration will be certified by the Florida Division of Elections in accordance with the Florida Voting System Standards.
- Voting station configuration seal: The Administration Board will verify and preserve the correct and secure configuration of the Voting Laptops before they are sent to the kiosk sites. This includes the hardware, software and associated materials. The preservation of the configuration once verified can be implemented by using tamper evident seals or lockers. In the case of software, a digitally signed copy of the software will be escrowed with the State Division of Elections and the Okaloosa County Supervisor of Elections.
- Kiosk configuration audit: During the deployment, voting, and decommissioning phases of the election, kiosk election officials will verify the integrity of the kiosk components – the Voting Laptops and the Voter Authentication Laptop. This verification process will consist at a minimum in the verification of the tamper evident seals and software fingerprints.
- In-person voter identification: The kiosk election officials will verify voter identity and eligibility before allowing the voter to vote.
- Paper record: Election officials will ensure that voters deposit the paper record in the secure receptacle before they leave the kiosk site.

#### ***11.1.2 Voter Authentication***

Voter eligibility will be checked by the kiosk election officials through a Voter Authentication Laptop connected to the Okaloosa VRDB through a secure VPN. The remote access to the VRDB and the security of the Voter Authentication Laptop will be adequately protected.

### **11.2 Data Centers**

One data center will host the VRDB and another will host the voting process. Each infrastructure will be accessed remotely from the kiosk sites through either the Voter Authentication Laptop or the Voting Laptop. In addition to the security measures implemented in the communication channel, appropriate security controls related to the access, management, and storage of the information in this infrastructure must be provided. The main security controls implemented for the voting and authentication processes are described below.

#### ***11.2.1 Voting System***

The voting system (server side) will be hosted in the voting servers located at a data center in Barcelona, Spain . These voting servers are managed by several persons with different roles, such as system administrators, communications administrators, and database managers. These personnel are not present in a traditional voting process and

will have privileged access to the system. Therefore, the security measures implemented in these systems must guarantee that the privileges of these personnel do not put at risk the election accuracy, availability and secrecy. Based on this principle, the following security measures are provided for this environment.

### ***Physical measures***

- **Restricted physical access:** Access to the voting servers will be physically controlled and registered. Only authorized persons will be able to access the room that hosts the voting servers.
- **Surveillance:** The data center will include video surveillance systems and the access to the server rooms will be controlled with access cards and keypads.
- **Tamper evident controls:** Servers, peripherals and connections will be protected by tamper evident seals or locks that will allow detecting any internal or external manipulation attempts.
- **Availability:** Voting servers will be redundant and have redundant components to prevent loss of service due to a component malfunction. Spare components will also be available for quick replacement in case of a component failure. Multiple copies and backups of the electronic ballot box are securely kept to prevent the loss of votes in case of storage failure.

### ***Logical measures***

- **Protection of the election configuration information:** The election configuration information used by the voting platform will be digitally signed by the Okaloosa Administration Board that validated it. The voting platform will check this digital signature to detect any manipulation attempts before starting the voting process.
- **Remote strong authentication of voters:** The voting server will only allow the remote strong authentication of voters.
- **Voter privacy:** The voting server will not have the ability to decrypt any received vote or stored vote.
- **Vote secrecy:** The encryption of the ballot preserves the secrecy of the vote.
- **Prevention of intermediate results:** Only the Canvassing Board can decrypt the ballots after the kiosk voting period is over and the ballots have been downloaded to the Mixing Server in Okaloosa County.
- **Prevention of coercion and vote buying:** Counted as cast receipt codes do not allow third parties to discern the voter's selections.
- **Ballot box accuracy:** Ballot integrity is protected by the voting protocol that integrates rigorous procedure and strong encryption technology.
  - a. Voters are physically identified against their voter registration record and a picture ID
  - b. They are issued a voting smartcard generated by the kiosk official that contains their unique PIN code and password
  - c. Only smartcards with valid PIN codes and passwords are accepted by the voting server
  - d. The smartcard creation system is rigorously protected to prevent malicious smartcard generation.

- e. Finally, the electronic ballot box is digitally signed when the election is closed to prevent any manipulation.

End-to-end security: The Voting Server will not have access to the encryption and decryption processes of the votes. Additionally, this server will not participate in the digital signature of the votes.

- Prevention of multiple vote casting: The server will not accept more than one ballot per voter.
- Vote loss prevention: The electronic ballot box will be stored in redundant media and backed up continuously to prevent the loss of votes in case of a system failure.
- Protection of the election audit information: The logs of the voting transactions will be protected by using immutable log cryptographic techniques. This technology links each new entry in the log with the previous ones by means of a hash function, and it digitally signs at a certain time interval (or number of entries in the log) the chained logs. Therefore, any attempt to tamper with the election logs will be detected and isolated.

### ***Procedural measures***

- Certification of the voting servers: The voting software running on the voting servers will be certified by the Florida Division of Elections in accordance with the Florida Voting System Standards.
- Protection of the voting server component integrity: After the certification of the voting platform, a digitally signed copy of the software will be escrowed with the State Division of Elections and the Okaloosa County Supervisor of Elections.
- Manual inspections of the hardware and software components will be implemented before, during, and after the voting process to detect any manipulation attempts of these components.
- Full election control by the Okaloosa Administration Board: The configuration and administration process of the election will be validated by this Board. This validation process requires digitally signing of any configuration information entered into the voting platform. The digital signature requires the collaboration of a pre-defined number of the Administration Board members. The voting platform components will verify the signature of any election information before accepting it.
- Strict access control of personnel with platform privileges: System managers and any other privileged personnel will have limited privileges in order to protect the election configuration and voting data. Access by the system manager and others to the platform components will be restricted to only the required areas.
- Infrastructure monitoring: All the infrastructure components of the data center (server systems, network infrastructures, firewalls, etc.) will be constantly monitored.
- Verification of election audit logs: The integrity of the immutable election audit logs will be checked periodically in order to detect any manipulation attempts.
- Secure decommissioning: All the election information and logs generated during the election will be backed up multiple times for redundancy in read only media. After verifying that the media can be read, the copies will be provided to the Okaloosa Supervisor of Elections. Disks and storage media used by the voting system during the election will then be erased , preventing any future access to this information.

### **11.2.2 Voter Authentication**

The Okaloosa County data center hosts the VRDB server. It will operate under the same security procedures which are currently in use for this system.

### **11.3 Okaloosa County Elections Office**

The Okaloosa County elections office is where ballot canvassing, decryption, and tabulation take place. This office will host the Mixing Server, the system in which all the cast ballots will be decrypted and the results report generated. Therefore, the security of this platform is of paramount importance to preserve the overall election accuracy and secrecy. Any manipulation of this server would pose a risk to voter privacy and election accuracy. To prevent this, the following security measures and controls are implemented:

#### ***Physical measures***

- **Tamper evident controls:** The server, peripherals and connections will be protected by tamper evident seals or locks that will allow detecting any internal or external manipulation attempts.
- **Off-line secure storage:** Once the Mixing Server has been configured and validated during the election setup process, it will be turned off and stored in the Supervisor of Elections secure vault during the election process, until it is required for the decryption and counting of the votes.
- **Air-gapping and isolated environment:** The Mixing Server will be located in the Supervisor of Elections secure vault with restricted physical access and with no network connections. All the data required to be imported/exported to the server will be uploaded/downloaded by means of removable media.
- **Availability:** The Mixing Server will have redundant components to prevent loss of service due to a component failure. Spare components will be available for quick replacement in case of a component failure.

#### ***Logical measures***

- **Restricted access to the Mixing Server:** Only defined users will be able to access the server.
- **Need for collaboration among the Canvassing Board members:** During the election configuration process, the private key is split in shares by means of a cryptographic secret sharing scheme and then destroyed. As a result of this process, the vote decryption process is not under the control of a single person since it requires the collaboration of a pre-specified number of the Canvassing Board members to reconstruct the private key.
- **Electronic ballot box accuracy:** Before starting the decryption process, the Mixing Server checks the electronic ballot box to detect any inconsistencies or tampering attempts. The Mixing Server checks the identity of the Bridge Laptop that downloaded the ballot box, the integrity of the overall ballot box, the verification that all the votes in the ballot box have been cast by valid voters, the presence of multiple ballots from the same voter, and the integrity of each individual ballot.

- Voter privacy: The Mixing Server will protect voter privacy after decryption by implementing a cryptographic mixing scheme. This process decrypts and shuffles the ballots to prevent any correlation between the decrypted ballot and the order in which it was cast. As a result of this process, it is not possible to correlate a decrypted ballot with the voter who cast it.
- Vote secrecy: The encryption of the ballot preserves the secrecy of the vote.
- Prevention of coercion and vote buying: In addition to the practices to preserve voter privacy, the counted as cast receipt codes retrieved from the ballots will also be shuffled. Therefore, it is not possible to correlate these codes with the decrypted ballots.
- End-to-end security: The election private key required to decrypt the votes does not exist until the Canvassing Board reconstructs it in the Mixing Server. Therefore, the Canvassing Board is the only entity able to decrypt the votes and proceed with the tabulation process.
- Non-repudiation of the decrypted votes and voter verifiable information: Once the votes are decrypted and the counted as cast receipt codes retrieved, both information sets are digitally signed by the Canvassing Board using the reconstructed private key.

### ***Procedural measures***

- Certification of the Mixing Server: The Mixing Server will be certified by the Florida Division of Elections in accordance with the Florida Voting System Standards.
- Protection of Mixing Server component integrity: After certification, a digitally signed copy of the software will be escrowed with the State Division of Elections and the Okaloosa County Supervisor of Elections.
- Verification of Mixing Server integrity: Under the supervision of the Canvassing Board, a member of the Administration Board will manually inspect the server and verify the fingerprint of the software to detect any potential tampering before the electronic ballot box is downloaded.
- Electronic ballot box integrity and authenticity check: The integrity and authenticity of the electronic ballot box and its contents will be checked by the Mixing Server before starting the decryption and tabulation process to detect and notify officials of any inconsistencies or tampering attempts.
- Full election control by Canvassing Board: Only the Canvassing Board can start the decryption and counting of the votes. The presence of any other personnel is not required during this process.
- Selection of Canvassing Board members: It is of paramount importance that these members have divergent interests to prevent collusion. Furthermore, a minimum number of members required to retrieve the private key is established to make collusion more difficult.
- Secure decommissioning: All the election information and logs generated during the election will be backed up multiple times for redundancy in read only media. After verifying that the media can be read, the copies will be provided to the Okaloosa Supervisor of Elections. The disks and storage media used by the voting system during the election will then be erased, preventing any future access to this information.

## 11.4 Communications

Finally, the security and availability of communications must be preserved to guarantee the access from the kiosk sites to the VRDB and voting servers. The security measures and controls implemented to accomplish this are described below.

### ***Physical measures***

- Strict access control measures to networking components: Physical access to network and firewall components will be restricted at all times.
- Redundant networked components: Networked systems will have redundant network connections to prevent the loss of communication in case of component failure.

### ***Logical measures***

- Secure and dedicated network connection: The communication between the voting kiosks and the VRDB and voting servers will be carried out through secure and dedicated virtual private networks (VPN).
- Strong authentication of the secure network connection: The VPN will be established using digital certificates on both ends, providing strong authentication.
- Firewall filter of connections: The VPN connections between kiosk sites and VRDB and voting servers will be restricted to the network addresses and VPN access protocol. This restriction is implemented at two levels: network firewall and system firewall. Therefore, no public access is available to these systems.
- Intrusion detection: Network sensors will be configured to detect any abnormal communication behavior.
- Alternative communication paths: VRDB and voting servers will have alternative connection addresses to switch the connection in case of a communication loss.

### ***Procedural measures***

- No use of DNS servers: The connections will not require the participation of any external server to resolve the addresses of the Voting Laptops and Voter Authentication Laptops at the kiosk locations or the addresses of the VRDB and voting servers. These addresses are kept undisclosed and, therefore, are not publicly available.
- Restricted network access: Network components and networked systems will be configured to fulfill only the minimum requirements to establish the VPN.
- Network monitoring: The network traffic will be continuously monitored to detect any suspicious behavior. Alarms will be activated in case any suspect activity is detected.
- Incident reporting: In case any attack attempt is detected, the origin will be communicated to incident response authorities (e.g., CERT).
- Contingency communication plans: Alternative communication paths will be configured for rapid cutover in case a problem arises with the primary path.