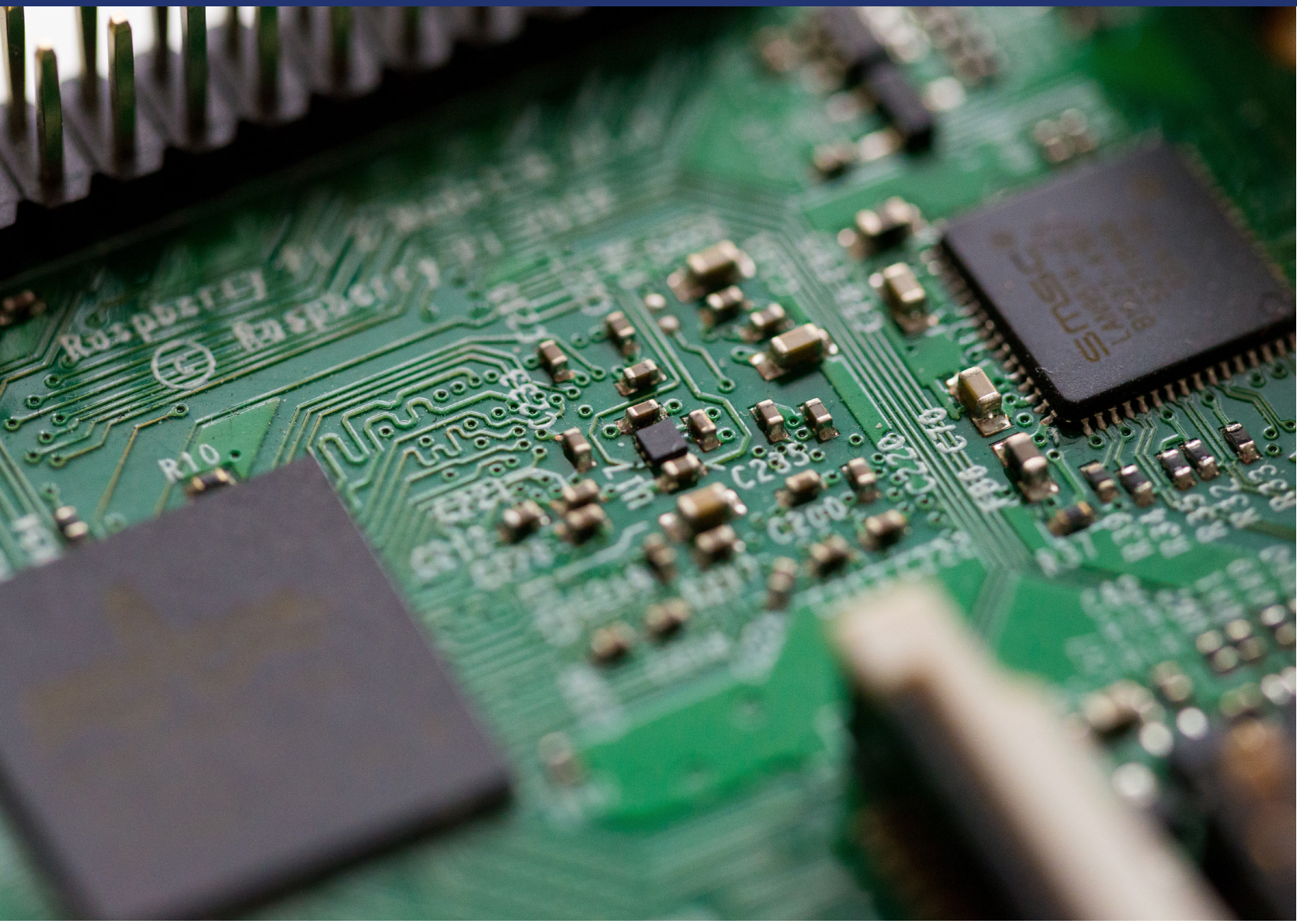
Global Expertise. Local Solutions.
Sustainable Democracy.

PRO V&V
VERIFICATION
VALIDATION

Pre-Election Assessment Report of the Dominican Republic's Automated Voting System



February 7, 2020

Pre-Election Assessment Report of the Dominican Republic's Automated Voting System

February 7, 2020

Pre-Election Assessment Report of the Dominican Republic's Automated Voting System

International Foundation for Electoral Systems
2011 Crystal Drive, 10th Floor
Arlington, VA 22202
Email: editor@ifes.org
Fax: 202.350.6701

Table of Contents

Introduction

From January 20-29, 2020, the International Foundation for Electoral Systems (IFES) conducted an assessment of the automated voting system that will be used in the Dominican Republic's municipal elections on February 16, 2020. This assessment was undertaken at the request of the Central Electoral Board (JCE) of the Dominican Republic and with the financial support of the United States Agency for International Development (USAID). This report documents the process and findings of the assessment that IFES conducted in collaboration with Pro V&V, a certified voting system testing firm based in Huntsville, Alabama.

The JCE had been developing the automated voting system for nearly a decade before it was used for the first time in the primary elections held by the Dominican Liberation Party and the Modern Revolutionary Party on October 6, 2019. Due to concerns raised following the October elections, the JCE agreed to engage an impartial, technically capable organization to assess the automated voting system ahead of the February 16, 2020, municipal elections. On November 28, 2019, the JCE sent a letter requesting IFES' support in collaborating with the United States Election Assistance Commission (EAC) to assess the automated voting system that will be used in the February 16, 2020, municipal elections.
In the February 2020 municipal elections, Dominicans will elect mayors, vice mayors and councilors in the 158 municipalities, and directors, deputy directors and district councilors in the 235 municipal districts. However, the automated voting system will not be used in every municipality. Automated voting will be used in 17 municipalities and the national district, which account for 9,757 polling stations and 62.04 percent of the electorate.[1] In the remaining municipalities, voters will use printed ballots to cast their votes, which will be transmitted to the tabulation center through a smartphone application provided to each polling station.

In accordance with the JCE's request and in an effort to enhance the transparency, credibility and trust in the 2020 elections, IFES contracted Pro V&V, Inc., on January 18, 2020, noting its certification by the United States EAC as a voting system testing firm.

The pre-election assessment conducted by IFES, together with Pro V&V, is neither an audit nor a certification of the voting system. It is a forward-looking evaluation of the automated voting system that will be used in the February municipal elections based on the assessor's expertise. The IFES assessment team, including Pro V&V, arrived in Santo Domingo on January 19, 2020, to evaluate the functionality and security of the voting system and provide short-, medium- and long-term recommendations to improve the voting system and its transparency.
Specifically, the assessment included an:

- Evaluation of the system's functionality
- Evaluation of the system's ability to keep voter anonymity
- Analysis of the auditability of the system

[1] The full list of municipalities using automated voting is included in Annex 3.

- Evaluation of the system's security features
- Analysis of the source code and stored procedures
- Evaluation of the system's ability to accurately capture voter intent

This report details the process, findings and recommendations of the pre-election assessment of the Dominican Republic's automated voting system.

Process Overview

The assessment team arrived in Santo Domingo, Dominican Republic, on Sunday, January 19 and began the pre-election assessment on Monday, January 20. The first step in the assessment was for the JCE to provide a detailed demonstration of the automated voting system. The assessment team was allowed to stop the demonstration and ask questions at its discretion. The assessment team found this very informative and received a good understanding of the system's inner workings from a technical point of view. The next step was to tour the production facilities and development environments on Tuesday, January 21.

The assessment team was then given a tour of the data center, development facilities, election materials production area and the warehouse used for collection, storage and distribution of the physical voting system components. On Wednesday, January 22, the assessment team started its hands-on assessment of the voting system by conducting interviews, reviewing the development environment and source code and examining configuration management practices and physical security. The assessment team was then provided two complete systems to analyze. This evaluation was performed on Thursday, January 23 and Friday, January 24. On Saturday, January 25, the team conducted a complete system integration test – from the unpacking and setup of the system to remote transmission of the results.

The assessment addressed each of the following goals in the manner described in the table below:

Figure 1: Assessment Overview

Goal	Summary
Evaluation of the system's functionality	The system functionality was evaluated by executing use cases for all system users, including technicians, officials and voters.
Evaluation of the system's ability to keep voter anonymity	Voter anonymity was evaluated by examining the voting process and the resultant data that was stored locally and transmitted back to the data center.

Analysis of the auditability of the system	System auditability review consisted of examining the logs produced locally and in the database at the data center.
Evaluation of the system's security features	System security evaluation included a review of the system access controls, physical controls, administrative controls, data transmission and encryption algorithms used.
Analysis of the source code and stored procedures	A detailed analysis of the development and build environments and a review of the database structure and stored procedures was performed.
Evaluation of the system's ability to accurately capture voter intent	The ability of the system to accurately capture voter intent was evaluated by verifying that compensating controls were in place to ensure a valid vote.

The basis of the assessment was the automated system, hardware, software and the technical documentation provided by the JCE. Figures 2 and 3, as provided by the JCE, depict the operational overview of the system.

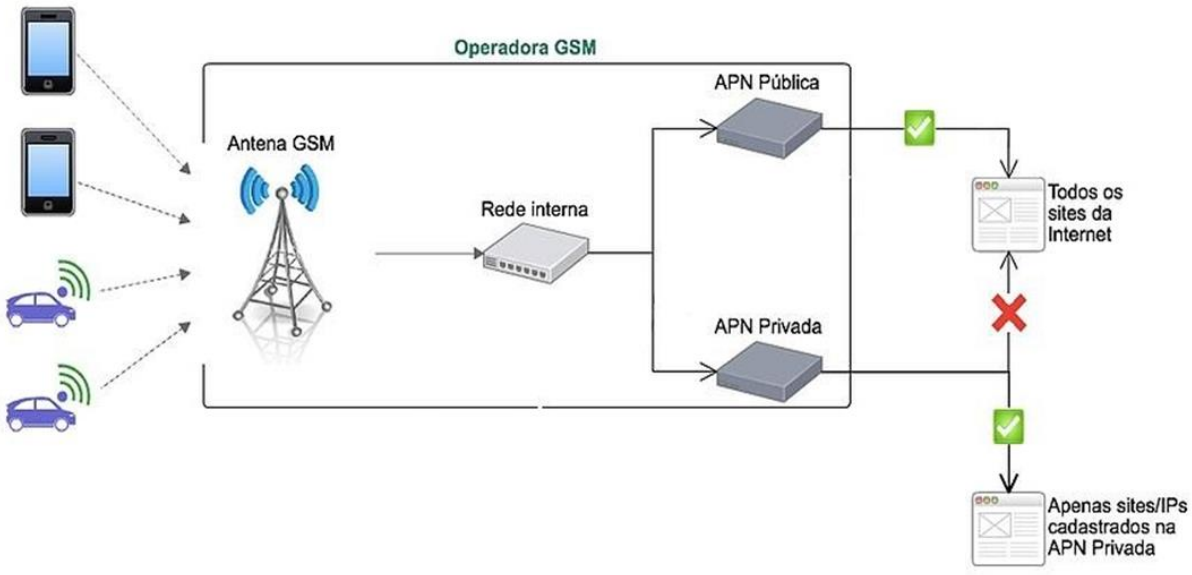


Figure 2: Operational Overview (Provided by the JCE)

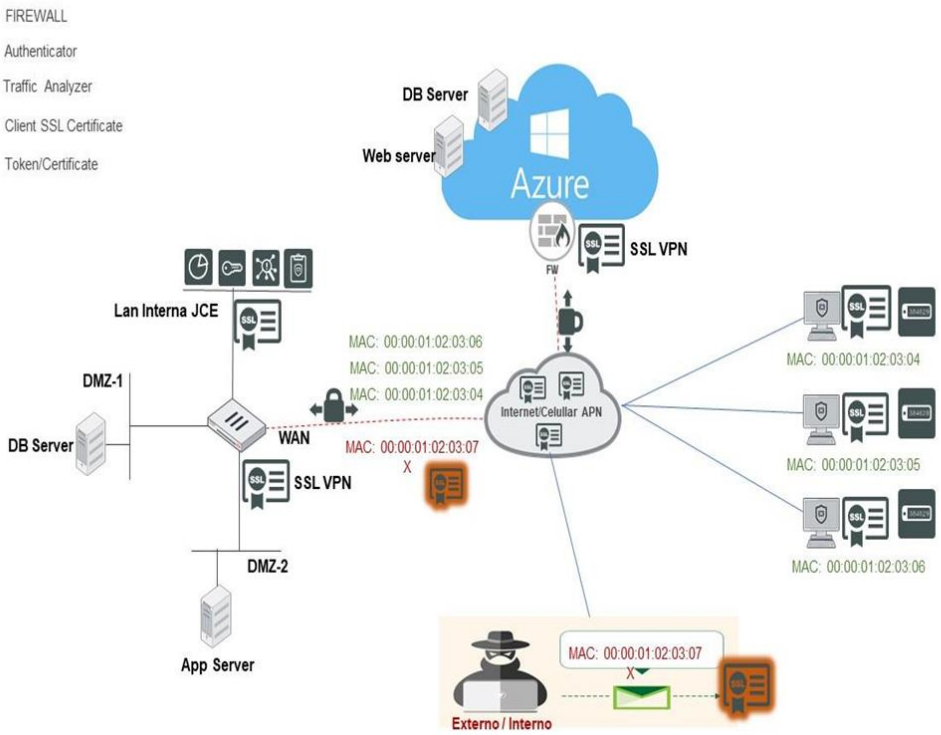


Figure 3: Operational Overview (Provided by the JCE)

Assessment Findings

System Functionality

The assessment team performed use cases[2] for all the roles that will interact with the automated voting system on Election Day. The roles include a maintenance technician who will set up the voting device, an election official who will check in voters, and the voter. These roles were examined in all three phases: pre-election, Election Day and post-election. The assessment team evaluators performed all features and functions allowed at each phase. This included calibration, machine diagnostics, opening of polls, voting and transmission of results. These use cases were performed using both positive and negative attempts to not only exercise the features and functions as intended, but to also exercise the voting device in a manner that was not intended. Some examples of negative testing would be placing letters or special characters in number fields, scanning different bar codes or QR codes, disrupting power during a voting session, connecting peripherals unknown to the system, disconnecting known peripherals, attempting to vote multiple times, attempting to undervote and disconnecting the transmission media.

In addition to the evaluation of the automated voting system's functionality outlined in the scope of the assessment, the team was asked to examine the smartphone app that will be used to transmit results in the polling stations that are not using the automated voting system. This examination focused on the input of both positive and negative data to ensure the device functioned as designed and was reliable enough to be used during an election. This examination was limited to only the post-election phase and the role of an election official using the device. The same techniques that were used on the voting system were also executed on the smartphone app.

IFES assessment team during the pre-election assessment from January 20-29

Conclusion

The assessment team found the architecture and overall design of the system to be of high quality and well executed. There were no defects, bugs or deficiencies found in the functionality of the automated voting system or the smartphone app that will be used in manual voting stations.

[2] In software and systems engineering, a use case is a list of actions or event steps typically defining the interactions between a role and a system to achieve a goal.

Voter Anonymity

The assessment team examined both the local voting device and the data transmitted back to the data center to try and ascertain if a voter could be tied directly to a specific voted ballot. The examination of the local voting device revealed that no logs contained any date or time stamps or voted data. Due to time constraints, the assessment team was unable to access the database locally because of difficulties presented by the system security. The assessment team focused on the data transmitted from the local devices to the data center.

The assessment team examined the results database's architecture and structure. Two tables were identified that contain voter information and voted data. These tables are electors_votar and votaron_x_elector, as described below:

- electors_votar – contains voter information on how a voter was authenticated and the method of authentication
- votaron_x_elector – contains the specific vote cast by table and machine ID

The only two common fields in both tables are IDmesa and IdProcessVotaron. Using these two fields in a query will only produce results of the machine and location information. A query could be constructed to show a voter did vote and where they voted, but not a specific vote. The unique vote is identified by the field IDVotaron, which is populated with a unique ID. Once another record is inserted into the table, all IDVotaron are randomly updated to another unique ID. This continues until the entire batch sent by the voting device is through processing. The last step is to randomly generate a new unique ID for the last record inserted.

Conclusion

The assessment team believes that this voting system does not store the information needed to retrieve a vote for a specific voter.

System Auditability

The assessment team evaluated the auditability of the automated voting system. This is defined as the ability of the system to record enough information to provide a certain level of confidence that someone other than the JCE staff can recreate the entire voting process. The information could be utilized to review the Election Day results and processes during a post-audit of the election to ensure all systems and processes were followed and accurate.

The assessment team examined logs for the operating system, database logs, logs from the device and other artifacts. The team was able to recreate the voting process with a high level of confidence. These logs provide date and time stamps for when events occurred. This information should be utilized in the post-election audit to create a timeline of the Election Day events and validate the results.

Another feature of the automated system is the ability of the JCE to monitor each device in real time. The JCE can see when a device is deployed, configured for the election and ready to transmit results. This allows the JCE to monitor that all systems are operating properly and to validate when all results have been securely transmitted. The post-election audit should verify and validate the communication of all deployed systems to ensure systems were operating properly and any issues were identified and logged.

The mobile app to be used in manual voting polling stations also provides real-time communication for when the app is opened and ready for transmission. In addition, the JCE can accurately track the smartphone dedicated to the polling location utilizing GPS coordinates, as the smartphones are dedicated to geographical locations. Should the device leave the dedicated geographical area a call may be placed to validate the reason for moving outside the area or to disable the device should the JCE believe it has been compromised.

Conclusion

The assessment team recreated the voting process with a high level of confidence, thus confirming that the system is auditable. However, as explained in the recommendations section below, creating a single "Audit Log," would improve the transparency of the system. The post-election audit should utilize all of the areas listed above to create a timeline of all events, verify the results and identify any areas for improvement or concern.

System Security

The assessment team evaluated the automated voting system's security features, including access controls, physical controls, encryption, encryption key management, encryption key creation and facilities security. Encryption and data transmission were particularly scrutinized.

The automated voting system uses eight encryption keys. The encryption keys are for each individual application or service running on the system. These encryption keys are RSA (Rivest-Shamir-Adleman) key encryption and are created by the JCE. Every election uses new encryption keys.

The automated voting system transmits results totals over the cellular data network. The JCE uses layered security to implement a secure data transfer. The first layer is that the payload is encrypted on the device. The second layer is that the payload is broken into packets and the packets are encrypted. These packets are then transmitted over an encrypted access point name (APN). The APN checks the media access control (MAC) address and SIM card of a device to see if it is a known device. If it is not a known device, it is dropped from the network. If the device is known, the transmission is sent to an IP address – a numeric designation that identifies its location on the internet – that is not public-facing and only known to the device and the APN. The third layer of data transmission security is the Network Admission Control (NAC). The NAC controls access to the network by MAC address and SIM card. The fourth layer of security is a firewall and network intrusion detection system. The fifth layer is the use of an application delivery controller. This ensures the transmission has the proper encryption keys to

connect to the correct server. The last layer of security is that the encrypted payload has to be decrypted using the private key on the server. The smartphone app used to transmit results in the polling stations with manual voting uses the same transmission media, encryption and network as the automated voting system.

Conclusion

The security features of the automated voting system and smartphone app are robust and follow best practices. An example would be the uses of the National Institute of Standards and Technology's (NIST) Security Content Automation Protocol and Center for Internet Security guidelines for baselining the operating systems used by the voting system. Pro V&V has no recommendation for the JCE in this area.

Source Code Analysis

The assessment team analyzed the automated voting system's source code. Because of the time constraints, the team could not perform a full function source code review as the voting system itself contains more than 250,000 lines of code.

The assessment team instead focused on gaining a high level of understanding of both the voting system and the application used by smartphones to transmit the results in manual voting stations and get a structural understanding of the source code. In addition, the team wanted to document the development environment as well as the build process and environment.

Figure 4: Automated Voting System Software

Automated Voting System		
Programming Language	Delphi	11.0.2709.7128
IDE	Adobe CodeGear	2007
Database	Server -Microsoft SQLServer 2017 Enterprise	
	Client – Microsoft SQLServer 2017 Express	
PC	HP Pro 400 G4 mini-PC with Microsoft Windows 10 LTS-C	

Figure 5: Mobile App System Software

Mobile App		
Programming Language	C Sharp	
IDE	Visual Studio .Net Framework	16.4.3 4.8.03752
Utility	Xamarin Forms	
Utility	Open CV	

The assessment team also believed the chain of custody for both the source code used to build the executable and the executable itself needed to be strengthened.

The assessment team obtained the MD5 hash and SHA1 hash values of the source code used to build the final version of the executable Pro V&V evaluated during the on-site assessment. On January 29,

2020, the assessment team joined the JCE via web conference to watch the final build to be used in the Dominican Republic's February 16, 2020, municipal elections. During this conference the developer and Pro V&V verified the hash values for the compressed source code. This code was then extracted and placed in the build environment. The developer update three encryption keys and the version number. The build was then performed. Immediately after completion of the build, a SHA256 hash was taken of the executable and an MD5 and SHA1 of the compressed code. Pro V&V then immediately transmitted the hash values to IFES. After the hash value was created and transmitted, the developer generated the detailed MD5 hash and detailed SHA1 hash for the individual files used during the build. Below are the hash values:

Figure 6: Hash Values

Urnavotacion_v3.0.0.0.rar	da57759ed862b6eabc7e9eedfa01effcf144957ec245a31fcc6012fe9a57f93a
SceUrnaVotacion.exe	df671d2f19925ae00424b706c56f42c98a78747aa3087b9485b71d892a81f1b82350cbd1

Conclusion

The development environment, configuration management and coding practices are sound. Improvements that can be made in these areas are included in the recommendations section below.

Voter Intent

The assessment team examined the automated voting system to determine its ability to accurately capture voter intent. The assessment team made attempts to undervote, miss hit target areas, repetitively hit target areas, select edge boundaries of target areas and try other techniques to see the response of the voting system. The automated system responded as intended. Instructions for voting in a proper manner are provided on each screen in clear text. The "cancel" and "confirm" buttons are always located in the same portion of the display. These controls provide for navigation forward and backward.

IFES assessment team tests the automated voting system's ability to capture voter intent

Conclusion

The assessment team believes the automated voting system contains sufficient compensating controls to properly capture voter intent.

Conclusion

The assessment team did not identify any major deficiencies in the automated voting system being used in the February 16, 2020, municipal elections. However, it did offer a series of recommendations that will improve the transparency and auditability of the voting system. Below are the short-term recommendations intended for implementation ahead of the February elections, medium-term recommendations intended for implementation ahead of the May elections and long-term recommendations to improve the voting system:

Short-Term Recommendations

1. **Address inclusion of polling station officials and political party representatives in two voter lists.** The current system as provided allows for the polling station officials – president, secretary, assistant secretary, etc. – and political party representatives to be in the voter list in two locations. The first location is the district where the official or representative resides and the other is where the official or representative is working. Because the officials and representatives are in the voter list twice, there is the possibility that they could vote twice, once in each location. While a simple search of the results after the election could determine if this occurred and for how many individuals, the assessment team recommends that the JCE either by regulation or by technical means address this issue before the February 16, 2020, municipal elections.

2. **Develop a new procedure for the use of the fingerprint scanner**. The automated voting system added a new fingerprint capture device that has not been used in previous elections. The assessment team observed many JCE employees vote in a mock election exercise. The team noted that everyone attempted to use only their index finger on their dominant hand. The assessment team recommends that the JCE develop a procedure for using different fingers if there is a problem capturing the first index finger. The team proposes that the procedure be to scan the index finger, followed by the thumb, followed by the ring finger on the dominant hand. If a fingerprint cannot be captured, retry in the same order using the nondominant hand. By attempting to use multiple fingers to capture the fingerprint, there may be more successful captures and fewer manual overrides. If the system fails to capture fingerprints from two consecutive voters, the poll station should contact the JCE for technical assistance.

Medium-Term Recommendations

3. **Select an escrow agent to hold voting system artifacts**. It is recommended that the JCE research and select an escrow agent to hold the final source code, executable, database and the accompanying hash value. The escrow agent may be the central bank, another government agency or a commercial software escrow agent. If an issue arises, or the election is called into question, the JCE can request that the escrow agent release the artifacts to a third party.

4. **Determine an amount of time before elections to halt system changes**. It is recommended that the JCE determine an amount of time before every election when development or changes to the voting system are halted. The amount of time before an election should be sufficient to allow independent third parties to review the source code.

Long-Term Recommendations

5. **Create a single audit log**. Although the assessment team was able to use the current logging for auditability, it recommends that the JCE compile the information into a single audit log for the deployed voting system. A single audit log that is human readable would improve the system's transparency.

6. **Develop a formal practice for tracking software defects**. It is recommended that the JCE develop a formal process for tracking software defects and that the JCE develop a formal software release process that includes change release notes. Best practices would be to have a formal process using tools that can communicate with more stakeholders.

7. **Automate the Secretary's Log.** It is recommended that the current Secretary's Log, which tracks all issues in the polling stations and is critical for a forensic examination, be automated. The current method of paper and pencil allows for changes and edits by simply using an eraser. An automated real-time system would ensure that no changes are made after transmission.

8. **Establish a formal software development process.** It is recommended that the JCE establish formal software development processes such as Capability Maturity Model Integration to formalize the processes and procedures used by the JCE in the development and maintenance of the voting system.

Annex 1 – References

Documents

- Letter from the JCE to IFES on the Electronic Voting System Assessment, dated November 28, 2019
- Elecciones ordinarias generales municipales del 16 de febrero del año 2020: instructivo electoral 2020 voto automatizado
- Elecciones ordinarias generales municipales del 16 de febrero del 2020: procedimiento para el escrutinio voto automatizado
- Elecciones ordinarias generales municipales del 16 de febrero del 2020: pasos para votar con el voto automatizado
- Election Assistance Commission *Testing and Certification Program Manual, Version 2.0*
- Election Assistance Commission *Voting System Test Laboratory Program Manual, Version 2.0*
- National Voluntary Laboratory Accreditation Program (NVLAP) *NIST Handbook 150, 2016 Edition*, "NVLAP Procedures and General Requirements (NIST Handbook 150)," dated July 2016
- National Voluntary Laboratory Accreditation Program *NIST Handbook 150-22, 2008 Edition*, "Voting System Testing (NIST Handbook 150-22)," dated May 2008
- Pro V&V, Inc. *Quality Assurance Manual, Revision 7.0*

Meetings and Teleconferences

- *Meeting, January 20, 2020 (JCE President's Office)* – The primary focus was the scope of the pre-election assessment. Attendees included JCE technical representatives, JCE leadership, USAID representatives, IFES representatives and Pro V&V assessors.
- *Meeting, January 24, 2020, a.m. (El Embajador Hotel)* – The meeting's objective was to inform stakeholders of Pro V&V's findings up to the final day. Attendees included U.S. Embassy representatives, USAID representatives, IFES representatives, Organization of American States representatives and Pro V&V assessors.
- *Teleconference, January 24, 2020, p.m.* – The teleconference's purpose was to provide stakeholders with Pro V&V's findings from the assessment. Attendees included U.S. Embassy representatives, USAID representatives, IFES representatives and Pro V&V assessors.
- *Meeting, January 24, 2020, p.m. (JCE President's Office)* – The meeting's purpose was to discuss the findings of the pre-election assessment. Attendees included JCE technical representatives, JCE leadership, USAID representatives, IFES representatives and Pro V&V assessors.

Annex 2 – Terms and Abbreviations

APN – Access point name

EAC – Election Assistance Commission

IFES – International Foundation for Electoral Systems

JCE – Central Electoral Board (Junta Central Electoral)

MAC – Media access control

NAC – Network admission control

NIST – National Institute of Standards and Technology

NVLAP – National Voluntary Laboratory Accreditation Program

USAID – United States Agency for International Development

Use Case – In software and systems engineering, a use case is a list of actions or event steps typically defining the interactions between a role and a system to achieve a goal

Annex 3 – Automated Voting Locations

Padrón Febrero 2020

4,644,590 7,487,040

62.04%

Municipio

Municipio	Recintos	Colegios	Electores	%
Total General	**1,772**	**9,757**	**4,644,590**	**100.00%**
DISTRITO NACIONAL	256	2,140	858,890	18.49%
SANTO DOMINGO ESTE	161	1,450	715,174	15.40%
SANTIAGO DE LOS CABALLEROS	218	1,194	591,545	12.74%
SANTO DOMINGO NORTE	117	639	350,601	7.55%
SANTO DOMINGO OESTE	87	514	271,943	5.86%
LA VEGA	114	442	213,211	4.59%
SAN CRISTOBAL	73	380	186,112	4.01%
SAN FRANCISCO DE MACORIS	109	367	173,266	3.73%
LOS ALCARRIZOS	67	305	166,463	3.58%
HIGUEY	91	322	160,395	3.45%
SAN PEDRO DE MACORIS	54	306	159,251	3.43%
MOCA	74	274	137,594	2.96%
LA ROMANA	54	285	133,148	2.87%
PUERTO PLATA	58	261	125,722	2.71%
BANI	47	249	118,944	2.56%
BONAO	60	242	115,270	2.48%
SAN JUAN DE LA MAGUANA	91	254	104,349	2.25%
MAO	41	133	62,712	1.35%

Annex 4 – Pro V&V Background and Qualifications

Pro V&V, Inc., is a software and systems test laboratory located in Huntsville, Alabama, USA. Founded in 2011, Pro V&V initially received its NVLAP from NIST on April 2, 2012. Pro V&V is accredited in voting systems testing for core test methods by NIST as part of the NVLAP and is accredited as a Voting Systems Testing Laboratory (VSTL) by the United States EAC.

Pro V&V brings extensive expertise and experience to the project, thus enabling the team to understand the objective of the assessment. Pro V&V's current staff, consisting of 13 full-time employees, is the most experienced in the industry, having performed testing for the majority of the completed EAC test campaigns to date. The Pro V&V team is comprised of members who are well respected within the voting systems testing community and possess a strong background in Independent Test Laboratory and VSTL voting systems testing experience. All employees of Pro V&V who are involved in test planning and execution are certified by the International Software Testing Qualification Board as Certified Testers, Foundation Level and are experienced in performing testing per the "V" Model as defined by IEEE to include Component, Integration, System and Acceptance testing, or possess demonstrable equivalent experience. Pro V&V is familiar and experienced with the use of IEEE 829-2008 Standard for Software and System Test Documentation. Additionally, multiple Pro V&V team members are credentialed in cybersecurity certifications.

Pro V&V core competencies include:

- Technical Data Package review
- Physical configuration audit, including examination of hardware components for safety, usability, accessibility, maintainability and operability of the equipment, and operational validation against user documentation
- Source code review, including coding standard compliances, security, build inspection and functionality
- Witnessed build and system installation testing
- Functional configuration audit, including the operational testing of hardware and software components and validation against user documentation
- System integration testing, including validation of accuracy, reliability, other high-volume tests and validation of processes and tools
- Telecommunication technology evaluation
- Security assessments of physical, administrative, technical and compensating controls

Global Expertise. Local Solutions.
Sustainable Democracy.

IFES | 2011 Crystal Drive | 10th Floor | Arlington, VA 22202 | www.IFES.org