LEGISLATIVE ASSEMBLY
FOR THE AUSTRALIAN CAPITAL TERRITORY

COMMITTEE SUPPORT

QoN No. 17

Standing Committee on Justice and Community Safety

Inquiry into Annual and Financial Reports 2022-2023
ANSWER TO QUESTION ON NOTICE

Asked by Mr Andrew Braddock MLA:

Reference: Hearing on 22 November 2023, Annual Report of the ACT Electoral Commission

In relation to:

Regarding the EVACS system:

(1) Why is the possibility of a voter believing that a print-out of their ballot doesn't accord with what they input into a voter screen treated as a risk to be managed, rather than as a potential source of system error to be addressed?

(2) If, at the next Territory election, a losing candidate were to challenge the validity of all EVACS ballots on the basis of it being impossible to verify that the vote database accords with voters' inputs, what would the Commission do?

(3) How does Elections ACT verify that the database of votes has only modified (added to) by valid and unique votes?

(4) How does Elections ACT demonstrate that the code running on the voting computers at an election was the same code as that made available for public inspection and without tampering?

Damian Cantwell AM CSC – ACT Electoral Commissioner: The answer to the Member's questions are as follows:–

Question 1:

The MLA's question is difficult to answer without additional context or clarity. This response addresses the apparent underlying issue of integrity assurance in the use of eVACS, specifically the proposal for a paper print out of the ballot cast being made available to an elector as a means of verifying the electronic vote.

The Elections ACT ICT Integrity and Security Assurance Plan, an Appendix of the Service Delivery Plan for the 2024 ACT Legislative Assembly Election, outlines the processes to be undertaken to assure the

integrity of the electoral ICT systems deployed by Elections ACT. Given the clear trend of voter preference for and confidence in electronic voting services as demonstrated in the 2020 election (more than 70% of all voters were cast electronically in 2020), Elections ACT considers it is very important to continue to transparently assure and demonstrate the integrity of eVACS in its preparation and deployment for the election, building on the inherently secure nature of the system due to its isolated LAN structure.

For the 2024 election, these integrity assurance measures will include:

- Continuous modernisation of the underlying software
- Independent auditing and certification of the software to ensure it contains no malicious code and operates as intended and that no votes can be added, deleted or amended
- Independent testing and verification of the functionality and reliability of the code
- Enhanced secure means of vote data transfer and multiple independent backups
- Public release of the code at least 6 months ahead of the election without the need for signing of a deed of confidentiality, to allow public scrutiny and testing of the code and any adjustments that may be necessary as a result
- External scrutiny of testing, and rehearsals of the system and related processes, including cyber incident response and recovery plans and rehearsals involving staff from Elections ACT, DDTS, federal security agencies and vendors
- Load testing under the most extreme possible operational conditions
- Infosec Registered Assessors Program (IRAP) assessment by an independent approved ICT security assessor against the federal Information Security Manual and Protective Security Framework
- Conduct of a Hazard and Operability Study (HAZOP) to identify and evaluate operational risks related to design of the system
- External eco-system cyber maturity assessments along with ongoing self-assessments utilising an externally endorsed process

As previously reported to the Assembly in this matter, the Commission considers the introduction of a paper verified vote arrangement is likely to unnecessarily raise integrity concerns with the voter, rather than achieve the purported aim of reassuring the voter that their vote has been correctly recorded. There are several operational issues associated with this proposal impacting on electoral integrity and trust:

- The need to add a secure printer to each voting terminal, along with the necessary conduct of individual integrity and assurance activities for each printer, would significantly increase operational complexity and risks to functionality, security, integrity and reliability of the system.
- The printers could jam, run out of toner or run out of paper. If this was to occur, it might not be

apparent to the voter whether a vote had been successfully stored on the server. Printer failure, or indeed an elector leaving with the printout, would also mean that any manual count would not duplicate the computer count. Scenarios such as this are likely to give rise to an elector's unjustified mistrust in the system.

- Establishing a printing arrangement that does not risk violating the principle of a secret ballot would be challenging and costly to implement. Each voting terminal would require a secure printer and a suitable secure and private location for its placement.

- It is not clear how it could be made possible for a voter to challenge a paper receipt if it did not accord with their memory of their electronic vote – presumably it would be important for a paper receipt not to be printed until after the vote had been stored in the server. The eVACS system already provides for screen verification prior to the vote being written to the server.

- A printed receipt would not, of itself, be proof that a person's vote has been recorded in the system as shown on the receipt. A means to verify this would be to conduct a complete check count comparing the printed receipts with the electronic vote count for any given set of votes. However, as discussed above, if the printed set of papers was not complete due to electors having departed or through printer failure, a manual check count cannot align with the electronic count.

- Conducting a full or partial manual hand-count using the receipts would be highly prone to errors. It likely that a hand-count of paper receipts would not be as accurate as the computer count. This would suggest the use of a receipt scanning system, similar to that currently deployed to count ballot papers but adjusted to accept the printed receipts rather than paper ballots. Introducing an electronic means of counting printed receipts would not be immune to the kinds of criticisms currently being raised against electronic voting and thereby not satisfying those with the concerns being raised.

The Commission considers that providing a paper receipt in addition to the current assurance measures in place unnecessarily and significantly increases operational complexity and risks to electoral integrity, does not enhance the verifiability of the eVACS, and would likely introduce undue and misplaced mistrust in the system.

Question 2:

The Commission does not agree that it is impossible to verify that the vote database accords with voters' inputs. The integrity assurance measures enacted around eVACS are intended to ensure that electronic votes are accurately recorded and that they cannot be lost or altered in any undetectable way. In particular:

- All votes are cast in a public polling place over an isolated local network.

- The Commission is an independent electoral authority responsible for the deployment of trusted and secure elections. In the case of eVACS, the deployment of a system designed to be transparent by making each step of voting and counting verifiable by public examination of the computer code. This is in stark contrast to the use of electronic voting in some other countries where electoral administrators are openly partisan and the code used in their proprietary systems is kept secret and in some cases not even provided for inspection by courts in the event

of a legal challenge.

- Voters are given an opportunity to review their votes, in preference order, before committing their votes to the 'electronic ballot box'.
- Votes are stored in the polling place server on two identical hard-disks.
- The voter does not receive the message saying "your vote has been accepted" until after the vote has been successfully written to the two hard-disks on the server – if the data is not successfully recorded the voter receives an error message that indicates the vote has not been recorded.
- The Graphical User Interface 'touches' are recorded during the production of a vote and are 'played back' in the system to ensure the vote to be recorded is correctly reproduced before the final vote submission.
- The software used in the polling place is independently audited program code that has also been made available for public inspections.
- Polling place servers are physically locked with physically restricted hardware that is monitored by independent electoral officials. Only trained and trusted polling place managers have access to the polling place servers, using two-factor authentication access, which only provides limited pre-defined functions through access to a menu. No other access is possible.
- Voting data is written to encrypted media at the end of each day's polling, with the data encrypted and identified by "hash" code information that is derived from the contents of the data – this data cannot be altered after the event without detection.
- System logs are auditable during and after the electoral event.
- The use of data encryption and hashing means a greater level of security is applied to electronic votes than to paper ballots.

If the result of the election was disputed in the Court of Disputed Elections, based upon a challenge to the validity of eVACS votes, the Commission would, with confidence, produce the auditable software code and system audit logs, together with providing the court with an understanding of the numerous assurance processes in place to ensure that the election result was an accurate record of voters' intentions.

Question 3:

The publicly available nature of the code, together with the engagement of an independent auditor to certify that the program does not contain code that unintentionally or maliciously alters the election outcome and separately also assessing that the code functions according to legislation, provides the Commission with appropriate assurance that the system captures, records and counts votes accurately.

Additionally, a review of system logs provides for an analysis of key system functions and system access to assure the Commission that no malicious activity has occurred during deployment.

Question 4:

The Commission will have the final eVACS source code for the 2024 election audited by an independent code auditor, scheduled for the first quarter of 2024. Following certification that the program does not contain code that unintentionally or maliciously alters the election outcome and functions according to the provisions within the *Electoral Act 1992,* the code will be made publicly available on the Elections ACT website.

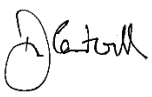
The certified version-controlled code will be formally notified by the Electoral Commissioner on the legislation register, identifying the approved code and version number as the code installed for use during the election.

The use of 'git' software configuration management and version control tool, used for the development of eVACS, is an important software procedure for comparing released code with deployed code. The 'git' tool uses hash codes for uniquely identifying each committed version in software development, including the final committed version to be independently reviewed, certified and ultimately deployed. This committed software package is immutable; unable to be altered. If concerns were raised with the software version deployed against the version certified for use by the Commissioner, an extraction process would be required to compare what was deployed against the immutable 'git' release.

System logs are also available to analyse to demonstrate that the installed software has not been accessed without appropriate authorisation and that key system components have not been altered during the event.

In addition to this, in 2024, as an additional integrity assurance and transparency measure, the Commissioner intends to make the code installation process a publicly viewable process. Interested stakeholders will be able to witness the installation of the original code on the official election server, which in turn produces the software image for creating and installing the polling place servers and voting terminals.

Approved for circulation to the Standing Committee on Justice and Community Safety

Signature: 

Date: 13 December 2023

By the ACT Electoral Commissioner, Damian Cantwell AM CSC