EXECUTIVE SUMMARY

On 5 September 2024, the auditor-general received a request from the minister of transport, Ms Barbara Creecy, MP, to audit allegations of tender process manipulation for the smart driver's card machine at the Driving Licence Card Account (DLCA) and its parent department, the Department of Transport (DoT). This followed widespread public concern over the appointment of IDEMIA South Africa (IDEMIA) as the service provider. The minister's communication was accompanied by a letter from the Organisation Undoing Tax Abuse (OUTA), in which specific allegations of an irregular procurement process were made.

It is worth noting that at the time of receiving the minster's request, the Auditor-General South Africa's (AGSA) auditors were already reviewing the specified tender as an early regularity audit process. The minister requested that we address the following focus areas in conjunction with the regularity audit processes:

- Whether the specifications in place for the project are adequate to protect the safety of personal data.
- Implications for the procurement process following the recent cancellation of IDEMIA's contract with the Airports Company of South Africa (ACSA).
- Whether IDEMIA's technical capacity and their ability to deliver key outputs timeously were adequately considered, especially following allegations of the challenges faced at three airports where IDEMIA's biometrics system has been contracted by the Border Management Authority (BMA).
- Whether South African service providers were considered in this procurement process.
- The affordability of the chosen bid.

To appropriately respond to the minister's request, we enhanced the proactive audit's initial scope to include additional procedures. In addition, to address all concerns raised and adequately respond to the risk, we deployed a multidisciplinary team consisting of forensic experts, information systems auditors and performance auditors to execute the specific additional procedures.

We audited Supply Chain Management (SCM) in accordance with the AGSA engagement methodology − as a result, we do not express an assurance opinion. The additional procedures executed fall within the mandate of the AGSA.

During the audit process, we identified instances of non-compliance with the required procurement processes and communicated these to the accounting officer and management. The non-compliances emanated from transgressions of SCM prescripts (Public Finance Management Act (PFMA), Treasury Regulations and DLCA SCM policies), rendering the procurement process irregular. The identified instances of non-compliance were due to:

- The DLCA's budget analysis, as part of the demand management process, being inadequate.
- Bids not being evaluated according to the evaluation criteria as per the bid specifications.
- Inconsistent application of scoring during the bid evaluation process.

Furthermore, during our assessment and discussions with management, we noted that the bid evaluation committee (BEC) deviated from assessing the bids using the exact criteria set out in the bid specifications when evaluating documents provided by bidders. The BEC members had to use their judgement and make executive decisions on how to assess the bids due to ambiguous bid specifications, which did not clearly address the DLCA requirements. This ambiguity led to discrepancies identified by the AGSA, resulting in an unfair and non-transparent procurement process.

The inconsistencies extended beyond technical evaluation to site visits conducted by the DLCA. During these visits, the DLCA was supposed to confirm that the machine proposed by the bidder, IDEMIA's MX8100, had the required capacity and capability to deliver on the requirements. However, the DLCA chose to inspect an unrelated machine. Management has not provided a satisfactory explanation or evidence for this decision.

The deviation from the bid specifications and the use of ambiguous criteria undermine the fairness and transparency of the procurement process. Furthermore, the evaluation of a machine not proposed by the bidder increases the risk that the selected service provider, IDEMIA, may not be able to fulfil the contract requirements. This could result in the DLCA failing to meet its constitutional mandate.

The tender was only awarded on 8 August 2024. While the current non-compliances

do not indicate fraud risk factors, their impact will be fully evaluated during the final regularity audit of 2024-25. At the date of this report, implementation and payment had not commenced.

Through this report, we aim to provide pertinent audit insights to the minister in response to her request. We strongly encourage the use of these insights and recommendations as a foundation to address the identified control weaknesses promptly and to ensure the timely implementation of the recommended corrective actions by the parties responsible.

2. CONCLUSION

Our audit of the DLCA's SCM processes revealed irregularities in the tender evaluation. IDEMIA, the winning bidder, failed to meet key bid technical requirements. Additionally, our review confirmed that the other bidders were not unfairly disqualified, as they also did not meet the bid technical specifications.

All bids submitted exceeded the R486,385 million budget set by the DLCA, indicating inadequate market analysis and budgeting. The DLCA used outdated pre-covid prices, and the budget they submitted to Cabinet for approval did not include all the costs for the contract, leading to Cabinet approving a memo that was not a true reflection of the cost of the contract. This poses the risk of the project being delayed or cancelled due to insufficient funds.

We also noted that the bid specification included an adequate assessment of the ability of the system to protect personal data. All bidders were evaluated on this criterion, and some were responsive.

We appreciate your proactive approach in assessing the procurement process for the card machine. We also commend the trading entity's positive attitude during the audit. We encourage the DLCA to perform continued oversight and strengthen SCM to prevent future issues.