1. Measures implemented.

- Appointed dedicated resource to manage information and cybersecurity.
- Approved information security policy in place.
- Firewall with intrusion detection and prevention capabilities to monitor & control incoming and outgoing network traffic based on predefined security rules.
- Anti-virus and Endpoint protection to protect all endpoints in our network against malicious software or programs.
- Advanced email and web content filtering system to block spams, phishing, and malware on emails; and restrict unsafe websites.
- Virtual Private Network (VPN) to allow officials to securely connect to internal systems when they are out of the office.
- Cyber security awareness (Security alerts, newsletters, phishing campaigns, awareness training) to train officials on how to recognize and avoid cyber threats.
- Vulnerability assessments to identify system weaknesses and thereafter remediation to reduce security risks and prevent attacks.
- Communication data encryption (SSL certificates) to protect sensitive information transmitted between end-users and departmental web-based systems for web services.
- Network security services (security gateway and email gateway) via SITA to secure departmental network against threats and unauthorised access

3. Measure intends to implement to enhance its cyber security posture:

- Review the security architecture as part of the Enterprise Architecture program which will inform the cyber security strategy to address the identified gaps.
- Implementation of advanced security tools as part on ongoing process to enhance the departmental cyber security posture.
- Enhance security resource capacity to enable continuous monitoring and response through skilled personnel or managed services.
- Encryption of all mobile devices.to protect sensitive data from unauthorised access in case of loss or theft.

- Continuous vulnerability assessments and penetration testing to identify and address security weaknesses.
- Continuous cyber security awareness training to keep officials informed about cybersecurity risk and best practices, reducing human-related vulnerabilities.

RTMC:

1) Breakdown of Incidents

An issue was reported on 18 January 2022 via the media that the online AARTO platform had unsecured endpoints which were revealing personal information. The service was taken off-line immediately and all endpoints were secured within 24 hours before the service was restored.

(1)(c)(ii) Over the past 5 years there have not been notable data breaches and ransomware attacks. There have been instances of cybercrime like phishing attempts which have been mitigated through the cybersecurity measures put in place.

(2) Current Cybersecurity Measures:

- Approved Cybersecurity Strategy and Implementation Plan
- Monthly tracking for accountability and progress

Approved Incident Response Plan (IRP):

- Ensures RTMC can effectively detect, contain, eradicate and recover from cybersecurity threats
- Regular updates to address evolving threats

Cybersecurity Controls:

- Use of security tools and appliances (Next-Generation Firewalls (NGFW) and Intrusion
- Prevention Systems (IPS)
- Anti-malware/virus protection
- Multi-Factor Authentication (MFA)

Cybersecurity Awareness Training:

- Simulated phishing attacks to train employees about cyber threats and best practices

Disaster Recovery and Business Continuity Plans (DRP/BCP)

- Redundant systems for critical services to minimize downtime:

- Regular failover exercises

(3)(b)(i)(ii) Planned Enhancement of Cybersecurity:

Measures	Timelines
Security Operations Center (SOC) with Security Information and Event Management (SIEM) & Security Orchestration, Automation, and Response (SOAR) capabilities.	2025/26 - 2027/28
Grey box penetration testing and vulnerability assessment.	2025/26 - 2027/28
Internal penetration testing, Vulnerability and Patch management.	2025/26 - 2027/28
Dark Web monitoring	2025/26 - 2027/28
Privileged Access Management (PAM)	2025/26 - 2027/28
Email security & continuity	2025/26 - 2027/28
Network Detection and Response (NDR)	2025/26 - 2027/28
Data Loss Prevention (DLP)	2025/26 - 2027/28
Zero Trust	2025/26 - 2027/28

The estimated cost for these initiatives is R12 000 000 per financial year.

SANRAL:

(1) The most recent data breach incident experienced by SANRAL occurred in 2014. This breach affected the online e-toll account management website. Subsequently, the organization implemented the PCI-DSS (Payment Card Industry Data Security Standard) compliance program, which is a global standard designed to ensure that all organizations storing, processing, or transmitting credit card information maintain a secure environment. This was part of the security improvement and monitoring plan to enhance its information security controls.

(2) SANRAL has implemented the following measures to improve information security controls:

- PCI-DSS Compliance program – This is a globally recognized security standard for organizations that handle credit card information. It provides a set of guidelines and

requirements to ensure that cardholder data is protected during transactions, storage, and transmission, ultimately reducing the risk of fraud and data breaches.

- Annual vulnerability and penetration testing – This enables the organization to proactively identify cyber security related weaknesses and implement remedial action to protect its IT systems from cyber threats.
- Security and Network Operations Centre (SNOC) – SANRAL has partnered with a reputable service provider for the provision of 24 x 7 security monitoring services to proactively monitor cyber security threats on behalf of the organization.
- Cyber security awareness program – Formalized employee cyber security awareness training to improve awareness.
- Appointment of key resources – SANRAL has recently appointed a General Manager (Chief Information Security Officer) who will lead the internal cyber and information security function and ensure that the organization follows best information security management practices.

(3) SANRAL aims to enhance its cybersecurity through the following measures:

- Establish an internal security function and recruit experts in the field.
- Review current ICT and cyber security strategy .
- Conduct security risk assessment to identify existing gaps and implement corrective actions.
- Modernize the security infrastructure and implement the latest technologies to improve SANRAL's security posture (e.g., AI, Machine Learning)
- Benchmark SANRALs information security program against peers for continuous improvement.
- Improve and entrench a cyber security conscious culture within the organization.
- Improve information security incident response and crisis management by conducting periodic simulation exercises.

The budget for all cyber and information security services including ICT risk management, IT governance and compliance is R400 mil over a period of five years.

RTIA:

(1) No data breaches, ransomware and cybercrime were experienced by Road Traffic Infringement Agency (RTIA) in the past five (5) years.

(2)

- Implemented a firewall for any incoming and outgoing traffic.
- Installed endpoint protection (Antivirus) and Endpoint Detection and Respond (EDR) Security
- Solutions.
- Encrypted computer hard drives, especial sensitive data.
- Regular updates of security patches and updates.
- Unique strong password and enabled Multi-Factor Authentication (MFA).
- Regular Cyber Security awareness sessions.
- Vulnerability and penetration tests.
- Implemented a disaster recovery and offsite backup storage.

(3) To continue improving on our current Security Solutions and benchmarking with the industry standards. Budget allocated for Cybersecurity:

No.	IT Initiatives	Budget
I	Renewal of Firewall	665,500.00
II	Endpoint Security	598,950.00
III	Encrypted Computer Hard drives	
IV	Regular Updates - Patch Management	477,650.00
V	Unique Strong Password and enable (MFA)	-
VI	Regular Cyber Security Awareness	-
VII	Vulnerability and penetration tests	1,210,000.00
VIII	Disaster Recovery	1,600,000.00
IX	Offsite Backup storage	174,240.00
	Total Budget	4,726,340.00

ATNS :

(1) ATNS experienced one (1) incident of ransomware that occurred in October 2023.

(2) ATNS has established a comprehensive cybersecurity capability with a skilled team incorporating advanced tools and stringent security controls to safeguard its systems and infrastructure. The organisation has deployed key security measures to ensure real-time monitoring, risk mitigation, and data protection, including:

- A Security Operations Centre (SOC) – A Security Information and Event Management (SIEM) system has been implemented to centralise security logs, analyse events, and detect anomalies in real-time, supported by 24/7 monitoring from a dedicated security team.
- Upgraded firewalls
- Security Awareness Training – Continuous education for staff on recognizing and mitigating cyber risks such as phishing, reinforcing a human-first defence strategy.
- Antimalware Solutions
- Multi-Factor Authentication (MFA) – Implementation of secure remote access protocols, requiring more than just a password to reduce unauthorized entry risks.
- Vulnerability Management System – Regular scanning for system weaknesses, identifying and addressing potential threats before they can be exploited.
- Data backups and recovery plans
- Endpoint security & encryption – Comprehensive protection for devices, including encryption measures to prevent data breaches if devices are compromised.
- Email protection – Implementation of filters and security tools to block malicious emails and mitigate phishing attacks.
- Network Access Control (NAC) – Secure access solutions ensuring only authorized users and devices can connect, reducing potential security breaches.
- Cybersecurity policies and compliance frameworks – Alignment with industry security frameworks, with regular audits and compliance checks to uphold cybersecurity standards.
- Through these security initiatives, ATNS reinforces its commitment to digital protection, operational resilience, and cybersecurity excellence, securing its infrastructure against evolving threats.

(3) To further enhance its cybersecurity framework, ATNS is rolling out a cybersecurity programme to improve its cybersecurity posture by investing on the following project:

Measure	Estimated Timeline	Estimated Budget
Incident response Improvement	2025/26	R1 000 000
Web application internal firewall	2026/27	R4 000 000
Identity and access management	2030/31	R15 000 000
Automated data leakage protection (DLP)	2026/27	R5 000 000,00
Penetration testing capabilities	2025/26	R1 000 000

Measure	Estimated Timeline	Estimated Budget
Security operations centre	2026/27	R14 000 000
Cybersecurity awareness training	2026/27	R5 500 000
Network access control	2029/30	R3 000 000
Network firewalls	2026/27	R8 000 000
Anti-malware	2027/28	R6 000 000
Vulnerability Management System	2029/30	R6 000 000

SACAA:

(1) One data breach occurred that was limited to one user's mailbox (b) N/A (c) N/A (i) (ii) at the South African Civil Aviation Authority (SACAA) in the past five years.

(2) The South African Civil Aviation Authority (SACAA) has implemented several robust measures to strengthen its cybersecurity posture and protect against evolving cyber threats. These measures comply with industry's best practices and regulatory standards such as POPIA and are continually reviewed and enhanced. Key measures include:

- Multi-Layered Security
- User Awareness Training
- Threat Detection and Monitoring :
- Incident Response Plan (IRP):
- Data Protection and Encryption:
- Identity and Access Management :
- Security Audits and Testing:
- Regulatory Compliance:

(3(a) To further strengthen its cybersecurity posture, SACAA has outlined several strategic initiatives aimed at improving threat prevention, detection, and response capabilities. A key priority is the full implementation of a centralized Security Operations Center (SOC), which provides 24/7 monitoring, threat intelligence integration, and real-time incident response. The SACAA also plans to adopt advanced AI-driven analytics to enhance anomaly detection, automate responses to low-level threats, and improve threat hunting capabilities.

Other planned enhancements include the deployment of Zero Trust architecture, increased investment in staff cybersecurity certifications, and stronger endpoint protection for remote and hybrid employees. Continuous user education improved third-party risk management, and regular cyber resilience testing will continue to form part of SACAA's proactive strategy to stay ahead of emerging threats and safeguard critical aviation infrastructure.

(3)(b)(i) The Security Operations Center (SOC), which provides 24/7 monitoring will be implemented effectively from 2025/2026 whilst both threat intelligence integration, and real-time incident response are planned for implementation in 2026/27 financial year

(ii) the total cost for the SOC is R6 million over 3 years, whilst the threat intelligence integration, and real-time incident response are estimated at R3 million collectively.

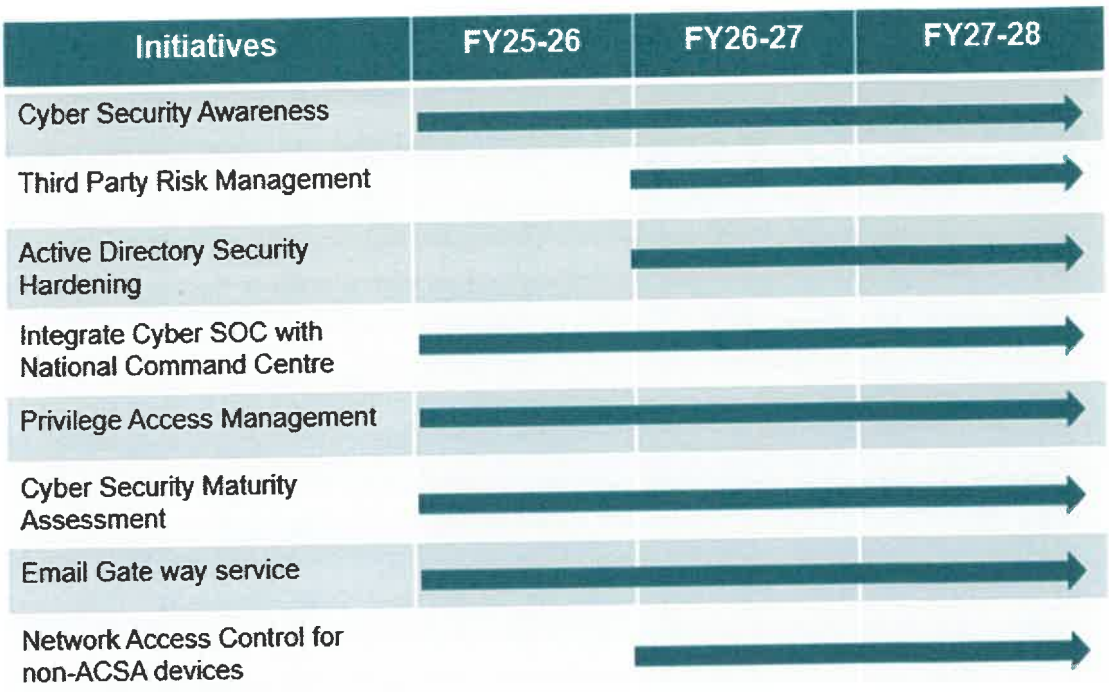
ACSA:

(1) There were no cyber security breaches in the past five years that required reporting to the relevant authorities in line with the relevant legislation.

(2) ACSA operates a mature Cyber Security Operations Centre (CSOC), with 24/7 monitoring, and rapid incident analysis and response. The SOC is the cornerstone of our breach attempts detection, protection and response. The SOC also provides threat intelligence and predictive analytics information. Information obtained from the SOC feeds into our everyday cyber security practices to continuously improve our controls. Our cyber security posture can also be described as mature and proactively managed. Some of our CSOC capabilities include threat intelligence, threat hunting, and external attack suffice management, amongst others.

(3) Our key priorities moving forward will be the rollout of our new 3-year cyber security roadmap. This will commence in FY25/26 with key priorities such as the integration of the cyber security operations centre (SOC) into the National Command Centre, implementation of the cyber security awareness platform, privileged access management, and next generation email security gateway. Other initiatives such as security hardening and third-party risk management will follow in FY26/27. This program will ensure that we take ACSA's cyber security capabilities to the next level.

Below is a summary of initiatives that will form our new 3-year program:



The table below outlines the summary of budget privisionsed for the three year period or cybersecurity telated exepenses.

Cost Category	FY26	FY27	FY28	Total 3 Year Budget
OPEX	R 4 086 562	R 10 381 134	R 9 873 334	R 24 341 030
CAPEX	R 4 986 000	R 22 992 392	R 1 000 000	R 28 978 392
Total	**R 9 072 562**	**R 33 373 526**	**R 10 873 334**	**R 53 319 422**

SAA:

(1) South African Airways (SAA) experienced no reportable data breaches, ransomware attacks, or cybercrime incidents over the past five years.

On 3 May 2025, SAA experienced a significant cyber incident, which was successfully contained within 12 hours by applicable business continuity mitigation protocols. The attack temporarily disrupted access to its website, mobile app, and internal systems. Core flight operations and customer service channels remained unaffected. The Digital Forensic Investigation team was unable to confirm data exfiltration definitively. However, ongoing dark web monitoring is still in place to identify any potential future disclosures or threats related to SAA.

As part of SAA's governance framework, the Audit, Risk and Governance Committee (ARCGO) of the Board receives quarterly updates on the integrity and sufficiency of the company's ICT systems.

(2) The theme of cybersecurity has always been at the top of the risk monitoring oversight of the Board. Human and technical resources have, over the period, been invested against cyber threats, and a general employee awareness training programme has been ongoing since SAA resumed operations in 2021. SAA was thus able to effectively activate its disaster recovery and business continuity protocols immediately upon detection of the cyber incident on 3 May 2025. The airline has reported the matter to the State Security Agency (SSA), South African Police Service (SAPS), and the Information Regulator in compliance with POPIA. Internal security teams and independent digital forensic experts are managing the investigation and response.

(3) Since the recent incident, SAA has initiated a dedicated project to strengthen its cybersecurity framework, including infrastructure upgrades, employee awareness, and system hardening.

Budget allocations are currently under review, with funding expected to be supported through internal resources and, where applicable, national security advisory support.

CBRTA:

1) (a) None

(b) Ransomware attacks: none

(c) Instances of cybercrime experienced: one (March 2021 - unauthorised and fraudulent telephone calls through the telephone PABX system)

(2) Measures implemented to protect the C-BRTA against cyberattacks:

- Implementation of the C-BRTA IT Cybersecurity Strategy
- Monitoring of cybersecurity risks through the strategic risk and IT operational risk registers
- Anti-malware software and monitoring and tools
- Encrypted access to IT systems
- Cybersecurity risk register
- Security vulnerability assessments
- Updated Information Security policy with cybersecurity framework and cybersecurity user awareness

- Annual Information Security Management Systems (ISMS) plan
- Third-party cybersecurity risk assessment tool
- Annual cybersecurity plan with budget planning
- Review of user access and administrator activities
- Implemented on-premise firewall and cloud web application firewall
- Disaster recovery plan and recovery services

(3) Measures the C-BRTA intends to implement to enhance its cybersecurity and the breakdown on the (i) timelines and (ii) budget allocated:

- Continuation with the implementation of the Cybersecurity Strategy
  - (i) Timelines allocated
  - (ii) Budget allocated
- Conduct security vulnerability assessments and implement security vulnerability assessment recommendations
  - (i) Timelines allocated
  - (ii) Budget allocated
- Implement the Information Security Management Systems (ISMS) plan
  - (i) Timelines allocated
  - (ii) Budget allocated

SAMSA:

a) There were no instances of data breaches experienced over the past five years.

b) SAMSA experienced two (2) instances of ransomware attacks in the past five years. The first incident was in 2021 and the second incident in 2023. The entity was able to recover from the two incidents through the backups and disaster recovery capability.

c) SAMSA had no instances of cybercrime over the past 5 years.

(2) SAMSA strengthened its security controls to improve the cybersecurity resilience through implementation of controls such as:

- Implemented the Next Generation Antivirus (CrowdStrike) with the capability of detecting and protection against potential security events/incidents.
- Regular review of firewall policies.
- Implementation of vulnerability management solution with automated patching.
- Review of backup security controls to ensure that backups are protected.
- Implemented the disaster recovery capability that is tested on regular basis (Bi-annually).
- Implemented Mimecast solution to protect the organisation against security threats via emails.
- Implemented the Security Operations Centre as a Service (SOCaaS) for proactive monitoring of the ICT environment.
- To ensure that all staff are trained on issues of security, the entity implemented the KnowBe4 security solution that provides scheduled training to staff on different security threats.

(3) The entity will continue to mature the implemented solution to ensure that the ICT environment is resilient against cybersecurity related threats. The following are the planned controls to be implemented includes and not limited to the following:

Planned Control	Timeframe	Budget Estimates
Zero Trust Network Access	FY: 2025/26	R 3 200 000
Cryptography Services	FY: 2025/26	R 5 000 000

RSR:

(1) The Railway Safety Regulator (RSR) has not experienced any data breaches, ransomware attacks, or instances of cybercrime over the past 5 years. The RSR continues to maintain a strong security posture through proactive monitoring, robust policies, and technical safeguards. These measures have ensured the ongoing protection of its information systems and infrastructure.

(2) The RSR continues to implement a multi-layered cybersecurity approach to protect against cyberattacks. This approach is underpinned by the implementation of effective administrative, technical, and physical ICT security controls, which include, among others, robust administrative policies, endpoint protection, firewalls, intrusion detection systems, and bi-annual cybersecurity awareness training for staff.

Furthermore, the RSR also performs regular patch management, penetration testing, and maintains encrypted backups to strengthen overall resilience.

(3) The RSR will continue to enhance its cybersecurity posture by expanding managed security services, incorporating artificial intelligence and automation into threat detection, and strengthening endpoint protection. Planned activities include ongoing upgrades to cloud-based security frameworks, extended user training, and additional penetration testing to ensure proactive risk mitigation. These measures will be implemented over the next 12 to 18 months, in line with the RSR's operational plan and cybersecurity approach. An amount of approximately R1.5 million has been budgeted for these initiatives for this financial year.

TRANSNET:

(1) Transnet experienced a cyberattack in the form of ransomware in July 2021. Transnet declared a force majeure as critical systems were not available for operations to continue.

Fortunately, since July 2021, Transnet has not experienced any data breaches, ransomware attacks, or cybercrime. In fact, in May 2025, the deployed cyber security tools detected malware in four servers and promptly contained the threat before it could spread further within the company's environment.

(2) Transnet remains committed to protecting its information assets and mitigating cyber threats by aligning with the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Oversight of the organisation's cybersecurity posture and strategic plans remains firmly with the Board, emphasising its importance at the highest level of governance. Transnet strengthened its cybersecurity capabilities through strategic interventions and advanced technologies, further enhancing it's resilience against an evolving threat landscape.

These capabilities include but are not limited to: Virtual Security Operations Centre (vSOC); Cybersecurity Awareness and Training; Continuous Vulnerability and Threat Management; Network Access Control (NAC); Network and Web Application Firewalls; Web and Brand Protection; Advanced Endpoint Protection solutions which employ advanced techniques and technologies (artificial intelligence and machine learning).

(3) Transnet recognises cybersecurity as a strategic enabler of both operational continuity and digital transformation. As a result, the organisation prioritises and enhances its cybersecurity posture through sustained investment in skilled personnel, advanced technologies, and robust processes. Transnet is modernising its legacy ICT environment with modern, high-performing digital technologies that are more secure. The technologies include but not limited to Software Defined Networks, Network Function Virtualisation, Hybrid Cloud Computing, and Advanced Analytics. These technologies leverages machine learning and artificial intelligence capabilities.

Road Accident Fund

(1) The RAF experienced two ransomware attacks in 2019 and 2021 respectively and one incident of unauthorised system access in 2024.

(2) The RAF has put ta 5-year roadmap in in place to implement cybersecurity controls across the environment. This is measured and reported at various Management and Board Committees. This roadmap includes optimising existing cybersecurity solutions as well as procuring additional cybersecurity controls. The following controls have been implemented to safeguard RAF from cyberattacks:

- Security Governance: Policies and and Standards
- Intensified POPIA training
- Network Firewalls
- Identity and Access Management (IAM)
- Endpoint Detection and Response
- Privileged Account Management Solution
- Cloud-Based Security Controls
- Centralised Identity Protection
- Vulnerability Management Solution
- Multi-Factor Authentication
- 24/7 Cybersecurity Monitoring
- Internet Security Controls
- Centralised Security Reporting Tool
- Patch Management Solution
- Attack Surface and External Attack Surface Management and Threat Intelligence Platform

- Cybersecurity Awareness and Training Platform and Program

(3) The RAF is in the process of implementing Cybersecurity projects in line with the RAF's five-year Cybersecurity roadmap. The projects include;(list projects) These initiatives are in different phases of implementation and/or procurement, with an overall budget of R83 000 000 for the 2025/26 financial year.

PRASA:

(1) PRASA has been subjected to data breaches, ransomware and cyberattacks. None of the attempted attacks succeeded against PRASA, thanks to its robust defence system. To maintain its edge, the entity remains alert, recognising that these threats are becoming increasingly sophisticated.

(2) PRASA has adopted a defence-in-depth approach that integrates advanced detection technologies, stringent access controls, user awareness initiatives, and continuous monitoring by a real-time Security Operations Centre (SOC). Prasa has also established a partnership with a Security Operations Centre (SOC) provider certified by the State Security Agency (SSA), enabling access to a global knowledge base through its Security Information and Event Management (SIEM) system. This multi-layered strategy enables early threat detection, prevention, and response—minimizing the risk of data breaches, service interruptions, and reputational harm across the entity.

(3) The PRASA cybersecurity strategy is guided by zero trust architecture principles and is comprehensively managed through its Security Operations Centre (SOC) and Security Information and Event Management (SIEM) services. This strategy aims to deliver holistic cybersecurity coverage across people, processes, technology,\ and financial domains, aligned with industry best practices and frameworks and the Government-Wide Enterprise Architecture (GWEA) for South Africa. From a human capital perspective, the most significant residual risk lies in user training and awareness. To address this, the department has partnered with KnowBe4 to deliver tailored cybersecurity training and awareness programs.

On the process front, key policies and governance frameworks have been developed and updated, while the overarching cybersecurity strategy is in its finalization phase.

Technologically, PRASA is enhancing its perimeter defences through the deployment of AI-driven Next Generation Firewalls (NGFs) in collaboration with original equipment manufacturers (OEMs). Over the next three years, the department plans to invest more than R55 million to strengthen its cybersecurity infrastructure.

MS. BD CREECY, MP
MINISTER OF TRANSPORT
DATE: 18/06/2025