KEYNOTE ADDRESS BY

DR AUDRIN MATHE,

EXECUTIVE DIRECTOR,

MINISTRY OF INFORMATION AND COMMUNICATION TECHNOLOGY

AT THE NAM-CSIRT CONSTITUENTS' INDUCTION ENGAGEMENT

DATE: 14 November 2023

VENUE: Mercure Hotel

TIME: 08h00 to 13h00

- Chief Executive Officer of the Communications Regulatory Authority of Namibia (CRAN), Mrs Emilia Nghikembua,
- CRAN Executive Management and team,
- Esteemed Stakeholders,
- Members of the Media,
- Ladies and Gentlemen,
- Director of Ceremonies,

Good morning. I am encouraged to see you all here this morning as we at the Ministry of Information and Communication Technology (ICT) welcomes this NAM-CSIRT Constituents' Induction stakeholder initiative by CRAN. Your attendance here is confirmation that there is indeed great interest in cybersecurity and what it promises to deliver and achieve for all stakeholders concerned, particularly at a time when more Namibians are connected and have access to and depend on networks for information and communication, business transactions and e-commerce.

Director of Ceremonies,

Cybersecurity threats are becoming more erudite, resulting in financial losses and related risks. Namibia is not exempted from such risks, as we have observed a rise in occurrences of misuse of available internet platforms and networks by criminals to carry out cyber-attacks. These incidences interfere with digital participation and connectivity as well as the integrity of our nation's critical infrastructure and critical information infrastructure.

To address this and protect its economy and citizens' privacy, Cabinet approved the development of the National Cyber Security Strategy and Awareness Raising Plan. The strategy outlines modalities to safeguard the public's privacy, educate and create awareness, information sharing and collaboration on cyber security and cyber crimes.

To that end, earlier this year, the Ministry of ICT launched the Namibia National Cybersecurity Strategy & Awareness Raising Plan 2022 – 2027, themed "*A step towards Cyber resilience & Digital Security*". Another noteworthy accomplishment is Governments decision to establish a National Cybersecurity Incident Response Team, with CRAN at the helm. The response team will serve as a trusted central coordination point of contact for cybersecurity, aimed at identifying, defending, responding, and managing cyber threats. Government has increased its efforts to ensure digital transformation and meaningful connectivity for all citizens in Namibia. We, however, cannot speak about digital transformation if our cyber security framework is not adequate. Hence, I applaud CRAN for taking the initiative to commence the work towards the full operationalization of the CIRT.

As it stands, Namibia still does not have the requisite legislation, including policies and regulations needed to effectively tackle the challenges currently faced in cyberspace, nor facilitate the cross-country investigation, prosecution, and adjudication of cyber and

cyber-related crimes. Thus, the MICT has forthwith prioritized the adoption of contemporary and vigorous cybercrime legislation that is in line with international standards, which includes the Data Protection Bill, as well as the Cybercrime Bill.

With these instruments in place, Namibia will be better prepared, adept, and vigilant against the threats that include phishing attacks, ransomware, cyberbullying, and child online vulnerability. This will equally ensure that we are able to reap the benefits and economic opportunities as presented by the ICTs.

In the interim, we must promote responsible usage of the Internet and create awareness of fraud, identity theft, cyber predators, and cyber ethics. We must ensure that there is increased knowledge about cybersecurity amid growing threats and attacks; we must engage all citizens, (young and old), reduce risks and help foster a culture of cyber vigilance; and educate citizens on the importance of cybersecurity and personal data protection.

The CIRT is not a policing tool and will have no investigation powers, as that remains the role of law enforcement. The CIRT will thus not interfere with existing rights, but rather serve as a protection mechanism for consumers, business enterprises and the full digital value chain. The CIRT will coordinate response to cyber incidents in collaboration with concerned constituents and its operations will be carefully set out to benefit constituents. I, therefore, encourage all constituents to support the work of the CIRT.

This is a mammoth task, and it should not be left to MICT, CRAN or NAM-CSIRT, to achieve. We call on ICT stakeholders and interested partners to join us in establishing cybersecurity related platforms for collaboration and exchange for the online safety of all our citizens.

In conclusion, I wish you a fruitful engagement.

I thank you!!!