DECEMBER **2025**

THE FOCUS

ICASA Independent Communications Authority of South Africa

www.icasa.org.za

CONTENTS

The Focus newsletter was compiled by:

The ICASA team
Editor: Zanele K. Ntuli
Editorial Team: Ramasela Matlou, Josias Mathiba, Thabisile Hlongwane and Owen Ramoroka

Copy editing, layout and design:
NEWSTART COMMUNICATION

Disclaimer
The newsletter contains information about ICASA related matters, be it an announcement, notice, advise, instruction and/or reports. Should the information be given as an advice, it should be confirmed and verified by any party intending using it. Without prejudice to the generality of the foregoing, we do not represent, warrant, undertake or guarantee that the information in the newsletter is correct, accurate, complete or non-misleading. We will not be liable to you in respect of any special, general, indirect or consequential loss or damage. All our rights are reserved. Reproduction in whole or in part without written permission is strictly prohibited. The views expressed in thefocus@icasa are not necessarily those of the editor, editorial team or NEWSTART.

Editor's note

Welcome to the third issue of The Focus for the 25/26 financial year!

This quarter has been marked by meaningful engagements, both locally and internationally, highlighting ICASA's continued leadership in shaping the communications sectors. From the successful SMME 's Dialogue 2.0 to major contributions at global regulatory forums, our work remains centred on promoting innovation, consumer protection and equitable access to communications services.

As we approach the festive season, we place strong emphasis on safety, both online and offline. In this edition, we provide guidance on how citizens can protect themselves from SIM-card fraud, cybercrime and other digital scams that tend to spike during the holidays. We encourage all consumers to stay vigilant and make informed decisions when interacting online or accessing mobile services.

We conclude this issue with a focus on international highlights of key engagements and outcomes stemming from South Africa's role in several key meetings of the International Telecommunication Union (ITU).

As the year draws to a close, we extend our gratitude to our readers and contributors for their support and dedication, which have been instrumental in ensuring the success of The Focus newsletter.

Have a safe festive break, happy holidays and a wonderful, prosperous New Year!

EDITOR & EDITORIAL TEAM

BEWARE of sim-card fraud during the festive season

As the festive season approaches, so too does an increase in mobile-related crimes, such as sim-swap fraud and illegal number porting. During this time of the year, consumers take advantage of holiday deals on new phones and contracts. Unfortunately, this excitement can lead to lowered vigilance, leaving individuals vulnerable to scams.

UNDERSTANDING SIM-SWAP FRAUD AND ILLEGAL NUMBER PORTING

SIM-swap fraud and illegal number porting involve criminals gaining unauthorised access to your mobile number. They may spoof your number to target friends and family or take control of your number to intercept sensitive communications, including banking One-Time PINs (OTPs).

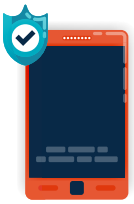
In some cases, unscrupulous mobile resellers or agents mislead consumers into signing agreements for "free" airtime or data on new SIM cards without complying with the mandatory registration process under RICA (the Regulation of Interception of Communications and Provision of Communication-Related Information Act).

These crimes not only disrupt the victims' lives but can also lead to a significant financial loss.

ICASA'S regulations to protect consumers:

- Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA).
- Number Portability Regulations of 2018.

Recipient-led processes are mandatory, meaning the consumer must initiate all port requests. Requests initiated by salespersons or third parties are prohibited.



ICASA reminds the public that mobile numbers cannot be ported without the consumer's request and approval through an OTP.

Update your contact details for alerts to your banking details.

TIPS TO PROTECT YOURSELF

ICASA recommends the following measures to safeguard against SIM-swap fraud and illegal porting:

Purchase SIM cards only from accredited service providers.

Secure your phone with a strong password and enable biometric authentication.

Monitor your phone's signal. Unexplained signal loss may indicate fraudulent activity – contact your service provider immediately.

Ensure all SIM cards are RICA-registered with accurate personal details.

Use a two-factor authentication (2FA) for all accounts linked to your SIM card, including banking, email, and social media accounts.

Avoid sharing personal information online, including your full names and mobile number.

Consider investing in security software to protect your mobile device.

SMME'S IN ICT DIALOGUE 2.0

"Advancing SMME's Participation in the Evolving Telecoms, Broadcasting and Postal Services Landscape"

SMME's in ICT Dialogue 2.0

ICASA successfully convened the 2025 SMME Dialogue on 03 December 2025, under the theme "Advancing Participation in the Evolving Telecoms, Broadcasting and Postal Services Landscape."

This year's dialogue followed the inaugural 2023 session, which provided SMMEs with a platform to raise key challenges affecting their ability to operate and grow within the ICT sector. Insights from that engagement have significantly shaped ICASA's regulatory focus over the past two years, particularly in areas such as Dynamic Spectrum Management, Infrastructure Sharing, Open Access and TV White Spaces.

The 2025 session reaffirmed ICASA's commitment to placing SMMEs at the centre of South Africa's digital transformation. During the engagement, ICASA provided updates on regulatory developments informed by previous SMME submissions. Participants discussed progress made in reducing regulatory barriers, improving fair access to spectrum and creating more competitive opportunities for smaller operators.

SMMEs acknowledged the positive shifts achieved to date, including efforts to open new avenues for participation in emerging ICT services and simplify regulatory processes. However, they also highlighted new and evolving challenges that reflect the rapidly changing digital environment.

ICASA further shared progress on initiatives designed to empower smaller players, particularly advancements in dynamic spectrum approaches and improved infrastructure-sharing frameworks. These developments were welcomed as essential steps toward lowering entry barriers. The open dialogue also allowed SMMEs to articulate challenges such as access to affordable infrastructure and navigating compliance requirements. Their insights will continue to inform ICASA's policy and regulatory work.

Cyber security tips:

As many people look forward to a well-deserved break, cyber criminals use this period to take advantage of increased online activities and holiday travels to target unsuspecting consumers.

Top Cyber Activities by Cyber Criminals:

Phishing, Vishing, Smishing

Social engineering scams used to steal money, sensitive and personal information (identity information, credit card details, banking information such as PINs or passwords) by sending malicious links via SMS or making fraudulent phone calls.

Online Shopping Scams

Fraudsters create fake e-commerce websites or malicious ads to lure shoppers looking for deals. Victims pay for goods that are never delivered or have their payment information stolen.

Common threats and security awareness:

Passwords

Passwords serve as a key to sensitive information on cell phones, laptops and other gadgets that Cyber criminals look out for.

Impersonation

Cyber Criminals send emails mimicking legitimate banks, retailers, or parcel delivery companies, often with “too good to be true” offers or urgent account related issues. These emails contain malicious links that lead to fake websites designed to steal personal and banking information.

Social Media Security

Criminals target victims with deals and offers that are illegitimate through social media. Criminals also search for any information posted by their victims about their whereabouts and current activities which are then used as part of the social Engineering attacks to scam and defraud victims

Public Wi-Fi

Often with the festive season, most people connect to public Wi-Fi around restaurants, retails shops and malls to perform quick and urgent payment and online activities. Cyber Criminals set up fake Wi-Fi that look similar to popular retailers and lure victims to connect to them and then intercept their online activities.

CONT...

What to do to keep safe:

Online shopping

- Be skeptical of festive deals, giveaways, or urgent prompts requiring private or banking details.
- Verify website authenticity and delivery messages before clicking links.
- Use multi-factor authentication (MFA) or two-step verification.
- Use a VPN to encrypt your connection when using public Wi-Fi on company laptops.

Physical shopping

- Avoid accepting assistance from strangers.
- Shield your PIN and stay alert for suspicious behavior.
- Keep your bag zipped and phone out of sight.
- Move to a crowded area and alert security if you suspect you're being watched.

Social Engineering Scams

- Don't announce travel plans on social media
- Confirm any bank or retail store offers by directly calling and checking for any changes or offers then agree to unsolicited calls and SMS claiming to come from bank or retails store.
- Limit who you share personal information with.
- Use your own data when performing sensitive online activities such as banking or payments.
- Criminals often know that most people travel during this time and use social media posts and updates to track whereabouts which can then be used for social engineering scams.

ICASA Q3 Highlights




Broadcating Workshop (Sandton)

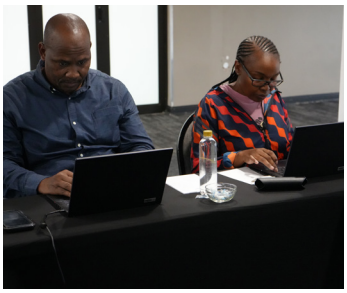


UJ Engineering and Built Environment Awards (Auckland Park)



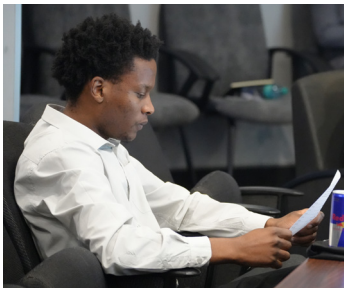

1st CRASA Electonic Communications Committee Meeting (Sandton)



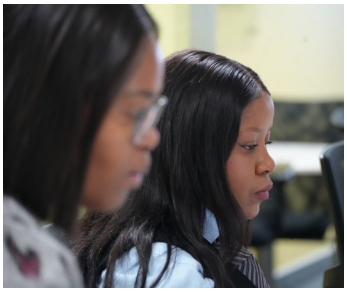



Council Strategic Session (Limpopo)






Public Hearings – Signal Distribution Regulations (Centurion Head Office)

Regulators Forum Roundtable Discussion (Centurion Head Office)

International Highlights - Key Engagements and Outcomes

The third quarter (Q3) saw international engagements covering forums that shape global governance, the future of the digital ecosystem and spectrum policy. South Africa played a prominent role in several key meetings of the International Telecommunication Union (ITU), including the Global Symposium for Regulators, the Working Party 7D, and various Council Working Groups.

ITU Global Symposium for Regulators (GSR-25)

The GSR-25 focused on the critical theme of "Regulation for sustainable digital development". The major tangible outcome of this symposium was the identification and endorsement of Best Practice Guidelines. These guidelines are designed to serve as a regulatory compass, encouraging regulators to transition their role from mere market overseers to proactive ecosystem builders.

The South African delegation was led by the ICASA Chairperson, who also served as a panellist. During the discussions, the Chairperson stressed that technologies such as satellites, fibre, wireless, and subsea cables should be viewed as complementary elements necessary for building a resilient digital ecosystem, rather than competing technologies.

Key regulatory demands emphasised by the Chairperson included:

- The establishment of integrated regulatory frameworks that actively promote convergence, infrastructure sharing, and partnerships.
- The necessity for transparent spectrum allocation.
- The use of innovative measures, such as regulatory sandboxes.

During the Heads of Regulators Executive Roundtable, a crucial consensus emerged regarding the need for regulators to cease operating in silos. Furthermore, there was a specific emphasis on the importance of incorporating youth, women, and persons with disabilities into future regulatory approaches. To bolster emerging technologies and develop solutions for SMMEs (Small, Medium, and Micro-sized Enterprises), strengthening partnerships with Innovation Fund entities was highlighted as crucial.

A major strategic objective for the South African delegation at the GSR was to utilise the platform to solicit international support for South Africa's African Telecommunications Union (ATU) Secretary-General (SG) for Ms Cynthia Lesufi.

ITU-R Working Party 7D (WP 7D)

The WP 7D meeting centered on Science Services and the vital protection of the Radio Astronomy Service (RAS). This focus is directly relevant to World Radiocommunication Conference (WRC-27) Agenda Item 1.16.

A primary and serious concern addressed at the meeting was the potential for interference posed by the emergence of Low Earth Orbit (LEO) satellites to the Karoo Central Astronomy Advantage Areas (KCAAA). To counter this threat and safeguard scientific assets, South Africa is actively seeking global protection through WRC-27 Resolution 681.

Given that the WRC-27 study cycle is currently halfway through, a significant threat was highlighted: the possibility of Agenda Item 1.16 resulting in a "No Change (NOC)" outcome. This failure could occur if critical characteristics of non-Geostationary Satellite Orbit (non-GSO) systems are not provided by relevant working parties. If this agenda item fails, South Africa risks losing the opportunity for the global protection and recognition of its Radio Quiet Zones (RQZs), which would have a detrimental impact on large-scale scientific endeavors, such as the SKA (Square Kilometre Array).

CONT...

ITU Council Working Groups and Expert Groups (CWGs/EGs)

This cluster of meetings addressed critical governance, financial, and policy issues across the ITU structure. South African representatives achieved key roles and contributed significantly to high-level discussions:

Ms. Cynthia Lesufi (South Africa) successfully chaired the 43rd meeting of the Council Working Group on the World Summit on the Information Society and the 2030 Agenda for Sustainable Development.

South Africa intervened in the discussion concerning the Headquarters Premises Project, formally requesting that the strategic risk register be presented to the CWG. This was intended to facilitate comprehensive monitoring of risk management strategies related to the project.

South Africa delivered a significant statement regarding developments at the African Network Information Centre (AFRINIC). The statement highlighted severe governance disputes and financial instability within the organisation, which are creating a systemic risk to the stability of the African internet. South Africa urgently called upon the international community to support an African-led, multi-stakeholder solution achieved through dialogue and mediation.

South Africa also utilised the forum to provide updates regarding its impending 2025 G20 Presidency. Priorities outlined for the presidency include key areas such as digital inclusion, AI governance and infrastructure development.

CONTACTS

CENTURION (HEAD OFFICE)

Phone: +27 (0)12 568 3000/1
Email: info@icasa.org.za

CAPE TOWN

Phone: +27 (0)21 561 6800

DURBAN

Phone: +27 (0)31 334 9500
Email: icasakzn@icasa.org.za

GQEBERHA

Phone: +27 (0)12 568 3060
Email: info@icasa.org.za

BLOEMFONTEIN

Phone: +27 (0)51 411 5900
Fax: +27 (0)51 447 3099

POLOKWANE

Phone: +27 (0) 15 001 0041
Email: limpopo@icasa.org.za

MAHIKENG

Phone: +27 (0)12 568 3251
Email: icasanwregionaloffice@icasa.org.za

KIMBERLEY

Phone: +27 (0)12 568 3042
Email: icasanc@icasa.org.za

NELSPRUIT

Phone: +27 (0)12 568 4054/2
Email: mpumalanga@icasa.org.za

Find us on the following social media platforms and website:
Twitter: @ICASA_org
Instagram: @icasa.za
Facebook: icasa.org
LinkedIn and YouTube: ICASA
Website: www.icasa.org.za

For Online Spectrum Licence and Type Approval Applications visit:
https://online.icasa.org.za/