Decisions on Recommendations (DORs) Matrix from the First of Two Rounds of Public Consultation on the *Guidelines for Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities*

The following summarises the comments and recommendations received from stakeholders in December 2024 during the first of two rounds of public consultation on the *Guidelines for Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities*. The decisions made by the Telecommunications Authority of Trinidad and Tobago (the Authority) have been incorporated in the second-round consultative document. The Authority wishes to express its thanks for all comments and recommendations received from the following stakeholders:

1. Ajmal Nazir.
2. Digicel (Trinidad & Tobago) Limited (Digicel)
3. Telecommunications Services of Trinidad and Tobago (TSTT)

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
1	General		Digicel	Digicel (Trinidad & Tobago) Limited ("Digicel") wishes to thank the Authority for the opportunity to provide its feedback on this consultation document. Please note that the views expressed herein are not exhaustive. Failure to address any issue in this response does not in any way indicate acceptance, agreement or relinquishing of Digicel's rights.	.	The Authority welcomes Digicel's comments and recommendations on this consultative document.
2	4.2	Network Security Monitoring and Detection	Digicel	We wish to highlight to the Authority that these measures will come at a cost to the business and creates a commercial implication or increment in the operating expense which may be borne by the customer.		The Authority acknowledges that the implementation of the cybersecurity guidelines may come at a cost to operators. However, the cost of a customer database breach or service failure

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						due to inadequate cybersecurity measures, with concomitant customer ill will and loss of brand reputation, should also be considered and a holistic approach adopted.
3	4.4	User and Network Interconnection	Digicel	"*Operators that allow application-based client access using Session Initiation Protocol (SIP) to public telephone services, either for business or residential users, are encouraged to use session border controllers (SBCs) (ITU 2015) and strong user and authentication credentials to mitigate the possibility of SIP clients being compromised. Operators should also ensure that customer premise equipment is maintained securely through appropriate patching and upgrades."* While it is essential for network operators to implement robust security measures, our obligations should align with what we can directly control and manage together with commercial feasibility considerations. For SIP services, we believe that operators should ensure a best-in-class setup, leveraging security features that fall within their operational and commercial scope and capabilities. This includes adhering to best practices, such as implementing secure configurations and enabling features that protect against potential risks.	Digicel recommends that any mandate for operators to use SBCs and other supplementary protections as a standard practice should be removed from this section as this would impose requirements beyond the operators' direct control.	The Authority advises that there is not any mandate that operators utilise session border controllers (SBCs) and other supplementary protections, however the section encourages their use. The Authority notes customers may choose their own solutions for Customer Premise Equipment (CPE). However, the Authority is mindful that session initiation protocol (SIP)-based services can be compromised, independently of the user device, as the operator's softswitch or SIP platform can be targeted directly. A customer-installed SBC will only mitigate the cyberthreat if the customer has a SIP platform on its premises. Therefore, as

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				However, the recommendations outlined on deploying SBCs, extend beyond the standard setup that operators can reasonably be required to provide. SBCs are supplementary tools (and typically offered as an add-on to the service) that enhance security by mitigating risks associated with SIP-based client access, but they are supplementary and intended to provide additional protection. The responsibility for deploying and managing such additional protections rests with the client, who must decide whether to invest in these enhancements based on their specific needs. While we can strongly encourage customers, the choice lies with them. Operators can have clients who choose to opt out of these optional add-ons to deploy their own solutions, making it clear that the final responsibility for implementing such advanced security measures lies with the customer. Operators can encourage and facilitate the use of SBCs and other supplementary protections, but mandating their use as a standard practice would impose requirements beyond the operators' direct control.		Digicel itself acknowledges, SBCs can provide additional security and should be encouraged. The Authority maintains its recommendation that operators should implement cybersecurity measures to protect its network and its subscribers' services.
4	4.5	Incident Report Capability	Digicel	We respectfully suggest to the Authority that the current definition of "incident" as it relates to incident response is excessively broad and creates an	The Authority is asked to define "incident" and to provide justifications or specified scenarios	As defined in the guidelines, incidents are events that either pose risk to a network or services,

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
		and Preparation		unmanageable burden for operators. There are no defined parameters of what qualifies as an incident, therefore, how do we determine a justification for limiting, throttling, filtering or blocking certain traffic flows.	for implementing such restrictive measures.	adversely affect the operation of a network or its users, or degrade services being provided, all of which have been captured in the definition of "incident" in the document. These are the parameters or criteria to be used to quality an incident for further intervention. The variety of services provided by telecommunications operators is broad and, with the ever-evolving technology, as well as the number and type of consumer devices and applications being utilised, it is impractical to define all specific or all possible scenarios of cybersecurity incidents.
5	4.6	Development and Maintenance of Cybersecurity Plans	Digicel	References to threat assessment of TT-CSIRT. Digicel maintains the view that this is an onerous request. The Concession speaks to the provision of information where the request is deemed reasonable. The request to submit these types of plans to the Authority in light of the existence of TT-CSIRT in the jurisdiction is also considered. We also wish to	The Authority is asked to clarify and specify the parameters it proposes for publishing and updating threat assessments.	The development and maintenance of cybersecurity plans by telecommunications operators are necessary, given the increasing number of cyberattacks and the effects of these cyberattacks on the

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				highlight the potential risk and reputational damage amongst other things if the information is mishandled or leaked. Further, where the annual update on plans has been provided, it needs to be clear how often these threat assessments will be published and updated by the Authority.		intended targets. The guidelines also state that the submission of suitable independent certification which verifies the existence of an operator's cybersecurity plan is also adequate. The publishing and updating of threat assessments are done by TT-CSIRT, not the Authority, and are done in accordance with the nature of the cyberattack that has been reported. Once the threat assessment has been updated and published by TT-CSIRT, operators are expected to review their cybersecurity plans, either annually or upon a major threat being identified, to ensure they are relevant to the assessment published, as stated in the guidelines.
6	4.7	Reporting of Cyber Incidents	Digicel	*"The Authority understands that, during an event, an operator's attention may be fully consumed with the mitigation of the cyber threat and the restoration of its services. However, operators are required to promptly notify the Authority of any cybersecurity incident.*	The Authority is asked to provide clear definitions, classifications, and conditions for what constitutes an "incident."	The Authority agrees with Digicel's recommendation that incidents that cause significant harm to services, users or network elements should be

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				Incidents may merely comprise attempts that were detected by their security detection and monitoring platforms and proactively extinguished before any network element or service was compromised, or constitute a full cybersecurity attack, where either services were adversely affected or impaired, or user or network elements were compromised by being infected with some form of malware, or inappropriate access was obtained." As stated above, we respectfully suggest to the Authority that the current definition of "incident" is excessively broad and creates an unmanageable burden for operators. The term, as drafted, encompasses both routine, proactively mitigated threats and significant cybersecurity breaches, which are fundamentally different in nature. Without clear definitions, classifications, and conditions for what constitutes an "incident," the requirement to report all such occurrences is impractical and could overwhelm both operators and the Authority with excessive, low-value reporting. To illustrate this, within our environment, thousands of "incidents" are triggered annually. However, under our internal policy, a vast majority of these do not qualify as actual incidents under company policy requiring	Digicel strongly recommends that only "incidents" that cause significant harm to services, users or network elements should be reported; to do otherwise, would be extremely onerous on operators.	reported, but would add that non-routine incidents that do pose a risk to services, users or network elements should also be reported. Section 4.7 has been amended to capture more explicitly which incidents need to be reported. The Authority agrees that there is no need to report on routine, proactively mitigated threats and cybersecurity attacks. The guidelines do not require Digicel to report to TT-CSIRT. The guidelines indicate that Digicel shall report incidents to the Authority; that the Authority may anonymise any reports received from operators; and the Authority may submit the anonymised reports to TT-CSIRT to ensure they are aware of ongoing cyberthreats in the industry. In terms of the guidelines related to secure information sharing, these are

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				escalation. These are largely routine events such as thwarted malicious attempts or system-generated alerts that posed no tangible risk to services, users, or network elements. Reporting every instance, as currently suggested, would divert critical resources from monitoring and mitigation efforts to administrative reporting tasks. Any robust cybersecurity infrastructure inherently detects and logs countless malicious attempts daily, as part of normal operations. Such attempts are not indicative of actual threats or compromises but reflect the effectiveness of detection and prevention measures. The lack of a precise definition in the current drafting makes it impossible to determine what should be reported, and broad reporting requirements risk desensitizing both operators and the Authority to incidents that truly warrant attention. In relation to the Authority's position that Digicel be required to be subject to reporting regimes to the TT-CSIRT, we are of the respectful view that we should not be compelled to submit to TT-CSIRTT as it is not within the purview or jurisdiction of the Authority to compel an operator to submit to another body.		only recommended. The Authority recommends that operators consider adopting in their own interest, as part of best practice observed in other jurisdictions such as Canada and Europe, but these guidelines are not mandated.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				In relation to Guideline 19, Digicel outright rejects any sharing of information with other operators as this would have major confidential and commercial risks to our operations.		
7	4.10	Cybersecurity Awareness, Education and Training	Digicel	*"25. Staff should be provided with all the tools necessary to fulfil their responsibilities while applying the company's cybersecurity protocols."* We acknowledge the importance of equipping staff with the necessary tools to fulfil their responsibilities while adhering to the company's cybersecurity protocols. However, "all the tools necessary" is overly broad and impractical. Instead, we propose that the requirement be reframed to reflect a more balanced approach, wherein operators commit to taking all necessary measures within the scope of available commercial resources to ensure staff are adequately equipped to support proper security protocols. The term "all the tools necessary" could imply an unbounded obligation that disregards the commercial constraints of the business, potentially leading to unrealistic expectations. Operators operate within finite budgets, and cybersecurity investments must be prioritized based on risk assessment, operational needs, and resource availability.	We propose a revision of this section, emphasizing that operators should take all reasonable and commercially viable measures to ensure staff are equipped with effective tools.	The Authority does not agree that the term "all the tools necessary" creates an unbounded obligation, as "being necessary" creates an appropriate bound for the provision. The Authority urges Digicel to reconsider its position as what is being proposed could create a situation where a tool that is necessary for cybersecurity protection is not deemed reasonable by an operator and then not provided. The Authority strongly encourages operators to provide their staff with the tools that are needed to protect their networks and customers' information.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
8	4.11	Monitoring and Compliance	Digicel	On the point of the failure of an operator to comply with a required guideline, Digicel questions the legality of this position. A policy guideline created by the Authority does not hold the same legally binding effect and/or legal obligation when compared to legislation or law as per the Telecommunications Act, Chapter 47:31 (as amended) and subsidiary regulations. Respectfully, Digicel is not of the view that a failure to comply with a policy guideline would constitute a breach of the concession.		The required guidelines are based on established obligations under the Telecommunications Act, Chap. 47:31 (the Act), the regulations, the concessions granted or other legislation in force, while Section A25 of the concession states that if there is any material breach of the Act, regulations, instruments, or directions made under the Act, or any conditions of the concession, the Authority, where appropriate, may take such action as it seems appropriate. In other words, the guidelines that are classified as "required" only reinforce existing legal obligations.
9	General		TSTT	Telecommunications Services of Trinidad and Tobago Limited ("TSTT") appreciates that the Telecommunications Authority of Trinidad and Tobago ("the Authority") has given operators the opportunity to comment on these matters. It should be noted that TSTT's comments on this document do not preclude TSTT from making further comments in the future.		The Authority welcomes TSTT's comments and recommendations on this consultative document.
10	General		TSTT	Legacy networks that are currently active and providing services to customers may not have been	TSTT suggests provisions be added in the guidelines to the effect that:	The Authority acknowledges that existing legacy networks may not

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				designed and implemented with modern cybersecurity risks in mind. Consideration should be given to the financial feasibility of replacing some legacy networks for the operator. *Notifying customers of any incident occurrence, timeframe for resolution* – Affected parties are notified as under law. Can TATT also clarify what is meant by this slide. Is TATT referring to throttling of network traffic?	"*While full compliance with all new cybersecurity standards is encouraged, the Regulator recognizes that the cost of upgrading certain legacy networks may be prohibitive. Therefore, operators of legacy networks are expected to implement an appropriate and cost-effective risk mitigation plan, demonstrating that they are addressing the key vulnerabilities in their legacy systems to acceptable levels*."	be equipped to incorporate measures that protect against cyberattacks. However, operators of such networks should implement guidelines that can be incorporated within their operation, which include, at least, the non-technical guidelines. For vulnerable aspects of legacy networks, the operators of such networks should indicate to the Authority how their adopted measures protect the relative parts of its network from cyberattacks. To reflect this approach of allowing legacy networks to be partially compliant with the cybersecurity guidelines, the following statement will be included in section 4.11, "Monitoring and Compliance'. *"While full compliance with all new cybersecurity standards is encouraged, the Authority recognises that the cost of*

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						upgrading certain legacy networks may be prohibitive. Operators of legacy networks, however, are expected to implement the Authority's guidelines that are applicable, while demonstrating that key vulnerabilities to cyberattacks in their networks are being addressed to acceptable levels, using appropriate measures, as part of their compliance report submission." In responding to a cyberattack, operators will have to mitigate the degradation of their service caused by the attack. The throttling of the malicious network traffic may be one method required to control the degradation of the affected service.
11	3.9	GSMA Baseline Security Controls	TSTT	The Authority is asked to note that GSMA Baseline Security Controls are related to FS.31 and not the Network Equipment Security Assessment Scheme (NESAS).	TSTT's recommendation is to revise the content of this section as follows, to avoid misunderstanding:	The Authority agrees with TSTT's recommendation and has revised section 3.9 by resituating the reference to the NESAS

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
					3.9 FS.31 GSMA Baseline Security Controls This document outlines a specific set of security controls that the mobile telecommunications industry should consider adopting. The solution description identifies specific recommendations that would allow operators to fulfil the control objectives. These controls are not binding and represent a voluntary scheme to enable an operator to assess and understand their own security controls. GSMA also develops and maintains the Network Equipment Security Assessment Scheme (NESAS) which provides a universal industry standard that acts as a security baseline against which vendors and their equipment can be tested and audited.	framework correctly within the section.
12	4.1	Protection of Critical Network Infrastructure	TSTT	TSTT notes that a concise definition of what comprises Critical Network Infrastructure is not provided. The Authority must define what constitutes Critical Network Infrastructure to ensure agreement among stakeholders.	TSTT recommends that there be agreement on the definition of Critical Network Infrastructure.	The Authority agrees with TSTT's recommendation and proposes to define Critical Network Infrastructure, as adapted from *the National Cyber*

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						Security Strategy and the ITU Global Symposium of Regulators Paper on *Cybersecurity: The Role and Responsibilities of an Effective Regulator* as "the vital networks, devices, systems or data that the incapacity of, destruction of, or interference with would have a debilitating effect on public safety or national security, or the provision of essential services directly related to the communications infrastructure of Trinidad and Tobago". This definition has been added to the guidelines under the Definitions section.
13	4.6	Development and Maintenance of Cybersecurity Plans	TSTT	The Authority states that "Under section 24 (1) (a) of the Act, a concessionaire is required to submit to the Authority for approval its plans in relation to its network development, quality of service and any other matter the Authority may require…". TSTT notes that cybersecurity plans are closely tied to network development and impact the quality of service provided by network operators. However, TSTT disagrees with	TSTT recommends that the cybersecurity plan be submitted to the Authority for informational purposes only, without requiring formal approval. The plan should remain adaptable to changes in the cybersecurity landscape without	The Authority refers TSTT to Guideline 14 which speaks only to preparing and submitting plans, as the Authority does not intend to delay an operator's adoption of its cybersecurity plan.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				the requirement that these cybersecurity plans, once developed in line with the guidelines, must be approved by the Authority. While TSTT is willing to share the cybersecurity plan with the Authority for informational purposes, we believe it should not require approval. As the Authority is aware, a cybersecurity plan involves more than just network development and includes elements that do not fall under section 24 (1)(a). Furthermore, TSTT understands that the Authority currently lacks in-house cybersecurity expertise to properly validate and approve such plans. Cybersecurity is a dynamic and evolving field, and plans should remain flexible to accommodate necessary changes without being hindered by the need for the Authority's approval.	delay or restriction from the approval process.	As these guidelines address securing of public tele-communications networks, if the elements of a cybersecurity plan that relate to network development or quality of service are inadequate, the Authority can advise the operator under section 24(1)(a) of the Act that those elements of their submission need to be revised. Guideline 14 has been amended to reflect the scope that falls explicitly under Section 24(1)(a) of the Act.
14	4.8	Supply Chain and Vendor Management	TSTT	TSTT notes the Authority's requirement regarding third-party vendors. However, TSTT has 1000s of vendors, and evaluating all of them is not practicable.	TSTT recommends that a clear definition be provided for categories of third-party vendors and the specific services they provide.	TSTT is asked to note that not all of its third-party vendors would be subject to risk assessments for the supply of goods or services that are vulnerable to cyberattacks. Section 4.8 speaks to significant vendor arrangements. Guideline 21 has been revised to reflect this criterion. The security layers within a network which are

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						affected by cyberattacks are the infrastructure security layer, the services security layer and the applications security layer (ITU-T X.1205). For vendors who supply goods and services relative to these security layers, cybersecurity risk assessments should be conducted and the necessary security measures implemented.
15	4.8	Supply Chain and Vendor Management	TSTT	The statement "operators should: 1. define security standards for the procurement of systems, services, devices and software that comply with such standards that may be established by the Authority." is too general and broad. Additionally, any standard established should be in keeping with international non-aligned standards bodies.	TSTT suggests that in establishing cybersecurity standards, the Authority undertakes a transparent and participatory consultation process with affected operators. This will ensure that resultant standards are demonstrably necessary, reasonably achievable, and do not impose undue or disproportionate economic burdens on industry operators.	The Authority affirms that any standards it establishes will be developed in consultation with the affected operators, consistent with how the Authority has always developed its standards and are developing these guidelines. The Authority believes that its statement adequately reflects its views stated above.
16	4.11	Monitoring and Compliance	TSTT	Under monitoring and compliance, an operator may need to procure services and implement technological solutions to meet compliance requirements. Many operators, particularly those under the purview of the Office of Procurement Regulation, may be required to	The guidelines should include provisions allowing an agreement between the Authority and operators on an implementation timeline before	The Authority acknowledges that operators will require time to implement the guidelines. TSTT is asked to note that operators should submit a proposed

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				follow rigorous procurement processes together with implementation efforts, which could affect the timeline for remedial actions.	operators are deemed to be in breach of the guidelines.	timeframe over which their guidelines will be implemented. Section 4.11 has been revised to accommodate the establishment of these timeframes. The Authority will review to assess whether or not a timeframe is reasonable.
				TSTT notes the statement that "The Authority does not consider the status of compliance with the guidelines as confidential information but, rather, as information that should be known to consumers and may be published by the Authority." TSTT disagrees with this view and believes that such information should not be made public. It can potentially be used negatively to attack an operator's network, which could harm the operator's reputation and operations.	TSTT recommends that the status of compliance with the guidelines be treated as confidential information, only to be shared with relevant stakeholders, and not be made publicly available unless the operator voluntarily agrees to disclose it. This would help prevent misuse that could harm the operator's business interests.	According to sections 3 (c) (iii) and 3 (c) (iv) of the Act, the objectives of the Authority include providing for the protection of customers of telecommunications services and promoting the interests of customers in respect of the quality and variety of telecommunications services. By publishing the extent of operators' compliance with the guidelines, consumers are provided with information that would enable them to choose a service in relation to the protection of their interests.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						While the Authority will not provide details of the specific guidelines with which each operator has complied, the Authority will advise members of the public on the extent to which an operator is compliant with the cybersecurity guidelines on a summarised basis.
17	Appendix II	Template for the Reporting of Compliance with Cybersecurity Guidelines	TSTT	Several requirements under this compliance template may not have been assessed or catered for by operators. Therefore, the timeline for implementing the requisite changes to meet the compliance requirements should be agreed upon after discussion with the operators.	TSTT recommends that provisions for implementation timelines for compliance be included in the guidelines and agreed upon by operators.	As indicated under guideline 14, operators will be given a year to submit to the Authority their cybersecurity plan or evidence of its existence. Along with the cybersecurity plan, operators should submit a proposed timeframe over which the cybersecurity guidelines will be implemented. The Authority will then review to determine whether or not the timeframe is reasonable.
18	General		Ajmal Nazir	The Telecommunications Authority of Trinidad and Tobago (TATT) has outlined comprehensive guidelines for securing public telecommunications networks and broadcasting facilities. While	We recommend the following approach: 1. **Base Requirement**: Mandate ISO/IEC 27001 compliance for all public	The Authority thanks Mr Nazir for his comment. The Authority agrees and has identified ISO/IEC 27001 under

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				these guidelines are commendable, clarity and standardization within the telecommunications sector can be significantly enhanced by adopting ISO/IEC 27001 as the foundational framework. ISO/IEC 27001, an internationally recognized standard for Information Security Management Systems (ISMS), provides a robust and mature framework for managing cybersecurity risks. It inherently incorporates mechanisms for flexibility and continuous improvement, making it well-suited to address additional requirements specific to Trinidad and Tobago's regulatory environment.	telecommunications and broadcasting operators as the primary cybersecurity standard. 2. **Supplemental Guidelines**: Any unique requirements identified by TATT, not explicitly covered by ISO/IEC 27001, should be issued as supplementary directives. This ensures alignment without undermining the consistency and global credibility provided by the ISO standard.	guideline 1 as the baseline standard to be adopted by public telecommunications network operators and service providers. However, the Authority has been unable to determine any country that has mandated ISO/IEC 27001 compliance on telecommunications operators and would welcome information on regulators that done so. From the Authority's research, ISO/IEC 27001 is considered a voluntary standard that can be used to support compliance with related regulatory requirements. Therefore, as these guidelines are being introduced, the Authority will not mandate ISO/IEC 27001 compliance on public telecommunications network operators and service providers at this time but will monitor its adoption.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
19	General	General	Ajmal Nazir	The ISC² (International Information System Security Certification Consortium) is a globally recognized organization for cybersecurity training and certification, offering unparalleled expertise and resources. The ISC² Caribbean Chapter, as a regional representative, possesses in-depth knowledge of cybersecurity challenges and best practices relevant to the telecommunications sector in Trinidad and Tobago.	We recommend that TATT establish a relationship with the ISC² Caribbean Chapter to: 1. **Leverage Expertise**: Gain access to the ISC²'s vast pool of cybersecurity professionals and their specialized knowledge in securing critical infrastructure. 2. **Training and Certification**: Facilitate training and certification opportunities for telecom operators and TATT personnel to enhance skills in areas such as ISO/IEC 27001, risk management, and incident response. 3. **Collaboration**: Collaborate on cybersecurity frameworks and initiatives tailored to the unique needs of the local telecommunications industry.	The Authority welcomes collaboration with the ISC² Caribbean chapter in developing robust frameworks for managing cybersecurity in the telecommunications sector.
20	General	General	Ajmal Nazir		**Additional Recommendations for Telecommunications Cybersecurity** 1. Adoption of Zero Trust Architecture	The Authority notes the additional recommendations provided and advises: 1. This aspect is covered in general under sections 4.1 and 4.2 of the guidelines,

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						where the Authority does not prescribe specific approaches to securing network infrastructure.
					2. Implementing AI-Driven Security	2. Similarly, the Authority at this time will not define for operators whether they use AI for security; operators should determine what is in their best interest.
					3. Secure 5G Implementation, including Network Slicing Security, 5G-specific protocol security and IoT integration security.	3. Specific considerations for 5G implementation have been addressed in the Authority's published *Framework for 5G Public Mobile Telecommunications Networks*.
					4. Regulatory Alignment with GDPR for Data Protection, requiring operators to implement GDPR-aligned data protection measures.	4. The Authority specified under section 4.9 the need for compliance with data protection legislation in effect.
					5. Advanced DDoS Mitigation, including deploying scrubbing centres and utilizing BGP FlowSpec.	5. Denial of Service (DoS) attacks are addressed in section 4.2 without reference to specific technical solutions.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
					6. Encourage adoption of RPKI for Secure Routing 7. Network Function Virtualisation (Security) 8. Mandate adherence to GSMA NESAS Framework for vendors supplying critical telecom equipment and integrate NESAS audits. 9. Require operators to adopt Enhanced Subscriber Authentication, such as Multi-factor Authentication and Biometric Validation	6. This recommendation was covered under 4.1 as it relates to securing signalling traffic, but the Authority will amend this section to include explicit references to secure routing. 7. The securing of virtual network elements is covered generically under sections 4.1 and 4.2, as part of the securing of critical network infrastructure generally. 8. The Authority notes this recommendation and can address the matter under the standards to be defined by the Authority in section 4.8. 9. Enhanced subscriber authentication is recommended in section 4.3. However, strict requirements, as proposed, can exclude subscribers without appropriate devices,

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						so the Authority would not require such measures.
					10. Encourage Cross-Border Cybersecurity Collaboration by operators, such as participation in the ITU Global Cybersecurity Index	10. It should be noted that participation in the ITU Global Cybersecurity Index is done at country level, not at operator level.
					11. Ensure telecom operators comply with Data Sovereignty Controls	11. Data localisation is covered under section 4.9.
					12. Require Red Team exercises	12. Red team exercises are covered in general under guidelines 15 and 16.
					13. Develop Open RAN Security Guidelines and mandate security certifications for Open RAN components.	13. Open RAN is covered generically on a technology-neutral basis in terms of secure access under section 4.4.
					14. Cloud Security in Telecom, requiring compliance with frameworks like CSA STAR certification.	14. This is covered generically, under sections 4.1 and 4.2, as critical network infrastructure.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
					15. Operators should implement Enhanced Spam and Phishing Protections	15. This is addressed under section 4.3 without dictating the use of any particular technology.
					16. Promote the use of Blockchain for Fraud Prevention	16. This is addressed under section 4.1 without specifying to operators any particular technology or approach.
					17. Define and advocate for Security for Over-the-Top Services	17. This would be beyond the scope of this document which pertains to operators of networks and infrastructure.
					18. Align telecom incident responses standards with International Benchmarks for Incident Response, such as the NIST CSF.	18. The timeframes specified in the guidelines were drawn from global incident response frameworks. It should be borne in mind that the operators are part of a broader cybersecurity ecosystem and therefore cannot operate beyond what is in existence locally.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
					19. Mandate Disaster Recovery and Resilience Planning, including frequent testing. 20. Encourage telecom operators to integrate with national Subscriber Identity and Digital ID	19. Disaster recovery plans as it pertains to cyber security incidents are addressed under section 4.5. 20. The Authority welcomes this recommendation and will collaborate with the industry on the viability of such an integration once national digital ID systems are operational.