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

The following summarises the comments and recommendations received from stakeholders in July 2025 during the second of two rounds of public consultation on the *Guidelines for the Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities* (the Cybersecurity Guidelines). The decisions made by the Telecommunications Authority of Trinidad and Tobago (the Authority) have been incorporated in the final document.

Based on the comments received from the second round of public consultation, the document was retitled from "Guidelines" to "Framework". Notwithstanding this change, the decisions captured in this document may refer to "Guidelines" and "guidelines", as the comments and recommendations received referred to the document as "Guidelines".

The Authority wishes to express its thanks for all comments and recommendations received from the following stakeholders:

i. US Embassy
ii. Trinidad and Tobago Bureau of Standards (TTBS)
iii. Amplia Communications
iv. Michael A. Ramesar
v. Southern Caribbean Fibre (SCF)
vi. Digicel (Trinidad & Tobago) Limited (Digicel)
vii. Columbus Communications Trinidad Limited (CCTL)
viii Telecommunications Services of Trinidad and Tobago (TSTT)

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
1	4.7	Reporting of Cyber Incidents	US Embassy		We recommend TATT refine the definition of "cybersecurity incident" to include only non-routine events that materially impact the confidentiality, integrity, or availability (CIA) of telecommunications networks or services. This will help ensure reports focus on events of operational significance, reduce noise, and improve response quality. In addition, we recommend establishing tiered thresholds and standardized timeframes for incident reporting, modeled on global practices and international standards such as the EU NIS2 Directive and U.S. NIST guidance: • High-impact incidents (e.g., data breaches, service disruptions) should be reported within 24–72 hours; • Low-impact or informational events may be logged and reported periodically.	The Authority welcomes this recommendation from the US Embassy and agrees with the Embassy that reports should focus on events of operational significance that adversely affect telecommunications networks or services. Accordingly, the Authority has included the following sentence in the second paragraph of section 4.7: "Operators will be required to submit reports only on cyberattacks where services were either adversely affected and user information or network elements were compromised." Guideline, now measure, 18 also has been revised as follows: "For cybersecurity incidents where telecommunications networks or broadcasting facilities were compromised and services were

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
					This two-tier model enables TATT to focus on the most serious threats, reduces unnecessary administrative workload for operators, and ensures that the Authority receives accurate, relevant, and timely information to support national cybersecurity oversight.	adversely affected or impaired, operators shall submit an incident report to the Authority no later than five days after resolution where the incident is resolved within five days or, for incidents not resolved within five days, within seven days of the start of the incident. The report shall specify the nature of the incident, the services affected, the scope of the impact of the incident, their customer notification plan, the timeframe for resolution of the incident, and any other matter the Authority may reasonably require." The timeframe adopted for the submission of reports on telecommunications service disruptions is within five to seven days of the disruption. The Authority, however, will establish a 12-hour timeframe for the notification of a cybersecurity

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						incident, whether it was addressed at the threat stage or involved the compromise or degradation of a network or user element and service. Guideline, now measure, 17 has been revised to reflect this, as follows: "Operators of public telecommunications networks and broadcasting facilities shall notify the Authority within 12 hours of any meaningful cybersecurity incident that occurs, whether the incident was unusual and addressed at the threat stage or involved the compromise or degradation of a network or user element and service, or user information."
+2	4.8	Supply Chain and Vendor Management	U.S. Embassy	Supply chain trust is the cornerstone of national cybersecurity resilience. We urge the Authority to adopt a regulatory framework that prioritizes the use of trusted suppliers: suppliers that are from jurisdictions that		The Authority acknowledges the US Embassy's recommendation. Given Trinidad and Tobago's legislative environment, the

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				respect the rule of law and have recourse to an independent judiciary or mechanisms to challenge state surveillance or data access mandates. To support this, we strongly recommend TATT incorporate explicit supplier risk assessment requirements for all ICT procurements, including: • Evaluation of a supplier's legal exposure to coercive data access (i.e., where such a vendor operates under foreign surveillance laws without meaningful judicial oversight); • Supply chain transparency and secure-by-design development practices; • Non-affiliation with entities sanctioned for malicious cyber activity. References: NIST SP 800-161 for supply chain risk management ISO/IEC 27036 for supplier relationship security We also encourage registration under SCS 9001, a new global supply chain standard developed by the Telecommunications Industry Association (TIA). The standard can serve as a practical option for countries and their authorities to pursue trusted suppliers and effectively exclude untrusted ones from participating in a country's market competition. While full certification is still in early adoption, registration represents an accessible, internationally recognized step toward long-term alignment with global supply chain security		measures listed in section 4.8 urge operators to ensure that vendors meet the required cybersecurity norms.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				norms. (Note: Registration with TIA does not require public disclosure.) Codifying a high bar for supplier trustworthiness grounded in transparency, standards, and law will mitigate the risk and harm of cybercrime. It will also mitigate the risk of surveillance, sabotage, strategic coercion, and misuse by both state and non-state actors of Trinidad and Tobago's digital infrastructure. Finally, it will also enhance the resilience of Trinidad and Tobago's digital infrastructure and promotes public confidence and investment from global technology partners.		
3	4.6	Development and Maintenance of Cybersecurity Plans	U.S. Embassy		We encourage a two-tier approach whereby: • All operators submit cybersecurity plans to TATT for record; • Only high-risk or Tier 1 operators are subject to formal audit or third-party validation. This preserves TATT's oversight role while encouraging operational agility and industry participation.	Currently, the Authority has not established a tiered approach for the regulation of telecommunications operators. To maintain that level playing field, all operators of public telecommunications networks and broadcasting facilities will be required to submit cybersecurity plans, or certification stating that the plans exist, to the Authority for review. The option to submit certification stating that the plans exist may make it less onerous on the major operators, as they may

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						be sceptical about submitting plans related to the security of their networks. The Authority acknowledges, though, that there is some merit in additional scrutiny for the larger service providers.
4	3	Relevant Global Cybersecurity Standards and Guidelines	U.S. Embassy		We encourage TATT to anchor technical expectations in globally recognized, supplier-neutral cybersecurity frameworks, including: • NIST Cybersecurity Framework (CSF) • ISO/IEC 27001 and 27005 • GSMA NESAS (with clarified application scope) • SCS 9001 (as noted above) This approach ensures international interoperability, protects against single-supplier dominance and getting locked-into obsolete technology, and promotes long-term resilience.	NIST Cybersecurity Framework, ISO/IEC 27001 standard and the Network Equipment Security Assessment Scheme (NESAS) are already referenced in the Cybersecurity Guidelines. A reference to ISO/IEC 27005 has been included in section 3.3. A new section, 3.9, referencing Supply Chain Security (SCS) 9001 has been included in the Cybersecurity Guidelines.
5	4.7	Reporting of Cyber Incidents	U.S. Embassy		TATT could play a central role in building secure, anonymized sector-wide information sharing—modeled	When a cyberattack incident report is submitted to the Authority, the information on the

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
					on U.S. Information Sharing and Analysis Centers (ISACs). This would enhance situational awareness while preserving operator confidentiality.	attack will be anonymised and passed on to the Trinidad and Tobago Cyber Security Incident Response Team (TT-CSIRT) to evaluate whether its threat assessment needs to be updated and also to inform other operators of the attack. TT-CSIRT performs the role of a centralised hub for the sharing of confidential information between operators and other entities whom the cyberattack may affect.
6	4.11	Monitoring and Conformance	U.S. Embassy	We appreciate the Authority's goal of using transparency to incentivize operator compliance and enhance consumer trust. However, we recommend that any rating system be designed carefully to avoid unintended consequences, such as discouraging incident reporting, oversimplifying complex risk profiles, or exposing sensitive security weaknesses.	As an alternative or complement, the Authority might consider non-attributed sector-wide benchmarking, combined with voluntary recognition for exemplary performers. This model harnesses market incentives while preserving a safe space for operators to report vulnerabilities, invest in improvements, and build resilience over time.	The Authority welcomes the recommendation of benchmarking operators' levels of cybersecurity compliance against a sector standard. When these guidelines have been implemented and matured throughout the sector, the Authority may then adopt benchmarking as a means by which an operator's level of compliance with the

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						cybersecurity guidelines is assessed and published.
7	4.10	Cybersecurity Awareness, Education and Training	U.S. Embassy	We recommend the Authority include language clarifying that all licensed operators and those operating under their license – to include affiliates, contractors, and subcontractors – are equally subject to the technical, procedural, and transparency requirements outlined in the Guidelines regardless of ownership, foreign affiliation, or government control. Uniform compliance standards are essential to ensure: • Fair competition within the telecom sector and advantageous terms for the citizens of Trinidad and Tobago • Risk parity across critical infrastructure providers, and • Credible enforcement of national sovereignty safeguards. This approach reinforces the legitimacy of the regulatory framework and supports investor confidence in a rules-based digital ecosystem, which will encourage greater foreign direct investment in technology in Trinidad and Tobago.		Operators cannot divest themselves of any of the responsibilities under the guidelines, by claiming it was their affiliates who failed to comply. These guidelines are for the operators and broadcasters to conform to, and it is their responsibility to ensure that their affiliates, contractors and subcontractors uphold the guidelines.
8	General	General Comment	TTBS	Would regulations for cybersecurity be necessary to ensure compliance by operators of public telecommunications networks and broadcasting facilities?	Considering the complexity of this topic, the potential impact on stakeholders, and the legal and operational issues outlined above, it may be useful for TATT to engage further with stakeholders based on the	Given the complexity of cybersecurity, the Authority held a pre-consultation with concessionaires on the proposed guidelines, at which time any reservations about meeting the

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
					comments and recommendations provided by TTBS.	requirements of the guidelines were addressed. The Authority, in accordance with its consultation procedures, then published the document for the required two rounds of public consultation, with this being the second round of consultation. The Authority is of the view that the pre-consultation, along with the standard two rounds of consultation, is sufficient, even when considering the comments and recommendations received from Trinidad and Tobago Bureau of Standards (TTBS) and other stakeholders from the second round of consultation.
9	1.3	Objectives	TTBS	Include national standards.	Revise to include - identifies relevant national, regional and global standards and recommendations that are applicable to the telecommunications and broadcasting sectors in Trinidad and Tobago.	The Authority agrees to include the term "national" and has revised objective 2 in section 1.3 of the Cybersecurity Guidelines accordingly.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
10	1.10	Objectives	TTBS	In order to avoid ambiguity, a clear delineation of voluntary guidelines and compulsory requirements should be made throughout the Guidelines. The terminology 'required guidelines' should be revisited as they are intended to function as compulsory requirements. Also, Good Regulatory Practices should be followed to establish compulsory requirements via the relevant legislation or within the relevant regulatory framework. In this regard, it may be useful to benchmark against legislation for cybersecurity in other jurisdictions.	Suggested rewording: voluntary recommendations and compulsory requirements	Clear definitions of the Authority's required measures and recommended measures are stated in section 1.10 of the Cybersecurity Framework. The required guidelines stated throughout the document are subject to existing obligations under the Telecommunications Act, Chap. 47.31 (the Act) or concessions. Section 3(c)(ii) of the Act, "The objects of the Act are to establish conditions for—promoting and protecting the interests of the public by—providing for the protection of customers," relates to the establishment of cybersecurity guidelines.
11	1.10	Conformance notation	TTBS	In order to avoid ambiguity, a clear delineation of voluntary guidelines and compulsory requirements should be made throughout the Guidelines. The terminology 'required guidelines' should be revisited as they are intended to function as compulsory requirements.	Consider the following changes: Required - compulsory requirements that the operator shall comply with fully. Recommended - voluntary recommendations that the operator is encouraged to adopt	These definitions of the Authority's required and recommended measures stated in section 1.10 of the Cybersecurity Framework have been used in previous documents written by the Authority and are therefore

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				Also, what is the legal mechanism that would be used by TATT to ensure compliance with a 'required' guideline?		consistent terminology. However, for clarity, the following statements have been included in the relevant parts of section 1.10 of the document: "A required measure is equivalent to a compulsory requirement." "A recommended measure is equivalent to a voluntary recommendation." The required measures stated throughout the document are subject to existing obligations under the Act or concessions. Failure to comply with any of the required measures will result in the Authority acting as prescribed under the concession or the Act.
12	3	Relevant Global Cybersecurity Standards and Guidelines	TTBS	As the National Standards Body according to the Standards Act No. 18 of 1997, TTBS should be mentioned here as it has adopted several International/ISO standards such as TTS/ISO/IEC 27001 and TTS/ISO/IEC 27002 which have been mentioned in Section 3.3.	1. Where applicable, the references to 'ISO/IEC 27001' and 'ISO/IEC 27002' standards should be updated to 'TTS/ISO/IEC 27001:2024' and 'TTS/ISO/IEC 27002:2024' respectively. Alternatively, an	The terms "ISO/IEC 27001" and "ISO/IEC 27002" throughout the document have been changed to "TTS/ISO/IEC 27001" and "TTS/ISO/IEC 27002", respectively.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				TTBS coordinates the national input into the development of ISO Standards and is a full member of ISO, representing Trinidad and Tobago's position in international standardization undertaken by ISO and IEC. Additionally, TTBS has declared the following National Standards pursuant to Section 16(4) of the Standards Act No. 18 of 1997. 1. TTS/ISO/IEC 27001:2024, Information Security, Cybersecurity and Privacy Protection - Information Security Management System – Requirements 2. TTS/ISO/IEC 27002:2024, Information Security, Cybersecurity and Privacy Protection - Information Security Controls 3. TTS/ISO/IEC 27003:2020, Information Technology - Security Techniques - Information Security Management Systems – Guidance 4. TTS/ISO/IEC 42001:2024 Information Technology - Artificial Intelligence–Management System 5. TTS/ISO/IEC 17788:2020, Information Technology - Cloud Computing - Overview and Vocabulary 6. TTS/ISO/IEC 17789:2020, Information Technology - Cloud Computing - Reference Architecture	undated reference can be utilised, such as 'TTS/ISO/IEC 27001' and 'TTS/ISO/IEC 27002'. 2. Content should be included within the Guidelines to indicate that TTBS has already adopted ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27003 as Trinidad and Tobago Standards pursuant to the Standards Act No. 18 of 1997. Include a paragraph on TTBS' role and Trinidad and Tobago Standards addressing cybersecurity, artificial intelligence and cloud computing. TTBS is the National Standards Body in Trinidad and Tobago, according to the Standards Act No. 18 of 1997. TTBS coordinates the national input into the development of ISO Standards and is a full member of ISO, representing Trinidad and Tobago's position in international standardization undertaken by ISO and IEC. Additionally, TTBS has declared the following National Standards	Section 3.3 of the Cybersecurity Guidelines has been revised to indicate the role of TTBS in the development of ISO standards and the adoption of ISO/IEC 27001 and ISO/IEC 27002 by TTBS as national standards, namely, TTS/ISO/IEC 27001:2024 and TTS/ISO/IEC 27002:2024, respectively.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
					pursuant to Section 16(4) of the Standards Act No. 18 of 1997. 1. TTS/ISO/IEC 27001:2024, Information Security, Cybersecurity and Privacy Protection - Information Security Management System – Requirements 2. TTS/ISO/IEC 27002:2024, Information Security, Cybersecurity and Privacy Protection - Information Security Controls 3. TTS/ISO/IEC 27003:2020, Information Technology - Security Techniques - Information Security Management Systems – Guidance 4. TTS/ISO/IEC 42001:2024 Information Technology - Artificial Intelligence–Management System 5. TTS/ISO/IEC 17788:2020, Information Technology - Cloud Computing - Overview and Vocabulary 6. TTS/ISO/IEC 17789:2020, Information Technology - Cloud Computing - Reference Architecture	
13	4	Guidelines for	TTBS	Correct ISO 27001 in the 2nd paragraph and within the text box.	Change ISO 27001 to TTS/ISO/IEC 27001	Throughout the document, the term ISO 27001 has been

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
		Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities				changed to TTS/ISO/IEC 27001:2024.
14	4.5	Incident Response Capability and Preparation	TTBS	With regard to incident response capability and preparation, will TATT be playing a monitoring and compliance role here?	It would be useful to outline the criteria for the approval of the incident response plan and monitoring activities.	The Authority does not intend to approve the cybersecurity plan but will review the plan to ensure that elements related to network development and the quality of service provided by network operators in relation to the mitigation of cyberattacks, such as the existence of an incident response plan, are in place. In addition, the Authority will ensure that proper notification and reporting of cyberattacks is carried out, in accordance with both the Framework and the operator's cybersecurity plan.
15	4.6	Development and Maintenance of	TTBS	What is the criteria for an independent certification ? It may be useful to reference ISO/IEC 27001 with regard to certification.	1) independent certification based on TTS/ISO/IEC 27001	Through measure 1, the Authority urges public telecommunications network operators and service providers

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
		Cybersecurity Plans		It may also be useful to indicate the certification/qualification requirements for professionals who are competent to review cybersecurity plans. Which entity will be the recognized cybersecurity authority? Which entity will provide the recognition or authorize the cybersecurity authority? Would legislation be necessary to authorize or create the cybersecurity authority?	Consideration should be given to the inclusion of a requirement for operators of public telecommunications networks and broadcasting facilities to be certified to the TTS/ISO/IEC 27001:2024 standard, where applicable.	to adopt TTS/ISO/IEC 27001 as the baseline standard. The Authority has been unable to determine any country that has mandated ISO/IEC 27001 compliance on telecommunications operators. From the Authority's research, ISO/IEC 27001 is considered a voluntary standard that can be used to support compliance with related regulatory requirements, inclusive of the regulatory environment in Trinidad and Tobago. Therefore, as these guidelines are being introduced, the Authority will not mandate TTS/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
						The intention is not to create a cybersecurity authority. TT-CSIRT is responsible for, and currently spearheads, cybersecurity responses and the restoration of operations affected by cyberattacks[1].
16	4.7	Reporting of Cyber Incidents	TTBS	If there is a cybersecurity incident, what are the penalties? How will these penalties be established? How will these guidelines work alongside other pieces of legislation (existing and future) addressing cybersecurity and cybercrime? Consider including timelines of reporting of cyber incidents. For example, Australia has a reporting time of 12 hrs for critical cyber incidents and 72 hrs for other cyber incidents. https://www.cisc.gov.au/resources-subsite/Documents/mcir-guidance.pdf	A system for financial and administrative penalties should be developed within the Guidelines, and by extension, within TATT's regulatory framework, for non-compliance with compulsory requirements (i.e. 'required guidelines' in the Consultative Document).	The Act does not prescribe administrative penalties. However, this is proposed in the amendments to the Act. Currently, concessionaires who commit a material breach of a concession obligation commit an offence and may face the penalties stipulated under section 65. Also, a breach of the Act can give rise to an offence under section 71 of the Act. The Authority can also recommend the suspension/ termination of the concession, in accordance with section 30 of the Act.

[1] Government of the Republic of Trinidad & Tobago National Cyber Security Strategy

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						The concessionaire is obligated to comply with all laws that are in force in Trinidad and Tobago, inclusive of any future cybersecurity legislation as may be applicable. This document is to be construed and interpreted in accordance with all national legislation. This document will be reviewed to ensure it continues to adapt to the needs of the telecommunications and broadcasting sectors and any modifications to the national cybersecurity legal and regulatory landscape.
17	4.8	Supply Chain and Vendor Management	TTBS	Add reference to standards issued by the Trinidad and Tobago Bureau of Standards. Add - ....standards defined by network operators and the relevant national authorities.	Bullet point 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 and the Trinidad and Tobago Standards as appropriate.	The Authority agrees with TTBS's recommendations and has revised section 4.8 accordingly. TTBS is asked to note that point 1 of section 4.8 has been revised to include the term Bureau of Standards, as follows:

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
					Bullet point 4 - establish procedures to ensure that vendors follow standards defined by network operators and the relevant national authorities. Bullet point 5 - support a verification programme to ensure that vendors, particularly of critical infrastructure, follow the standards defined by the network operators and the relevant national authorities	".....standards that may be established by the Authority and the TTBS". Point 4 of section 4.8 has been revised as follows: "4. establish procedures to ensure that vendors follow standards defined by network operators and the relevant national authorities, including the Authority and the TTBS." Point 5 of section 4.8 has been revised as follows: "5. support a verification programme to ensure that vendors, particularly of critical infrastructure, follow the standards defined by the network operators and the relevant national authorities, including the Authority and the TTBS."
18	4.9	Subscriber Privacy and Data Protection	TTBS	What are the penalties for non-compliance? For example, if there are data breaches, will there be financial penalties?	A system for financial and administrative penalties should be developed within the Guidelines, and by extension, within TATT's	As indicated above, the Act does not currently prescribe administrative penalties.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
					regulatory framework, for non-compliance with compulsory requirements (i.e. 'required guidelines' in the Consultative Document).	Concessionaires who commit a material breach of a concession obligation commit an offence and may face the penalties stipulated under section 65. Also, a breach of the Act can give rise to an offence under section 71 of the Act. The Authority can also recommend the suspension /termination of the concession, in accordance with section 30 of the Act.
19	4.11	Monitoring and Conformance	TTBS	With regard to Monitoring and Conformance, it is critical to ensure that there is no regulatory overlap with other national competent authorities with responsibility and oversight for cybersecurity.		The Authority accepts that there may be overlap, as these guidelines are meant to complement and not supersede other national regulations and policies that focus on the sectors the Authority regulates. 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 interest of customers in respect of the

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						quality and variety of telecommunications. The intention of this Framework is to mitigate the effects of cyberattacks on telecommunications networks, thus protecting customer data and promoting customer quality of service.
20		References	TTBS	CBTT. 2023. Cybersecurity Best Practices Guideline. Policy guideline, Port of Spain. https://www.central-bank.org.tt/sites/default/files/page-file-uploads/cybersecurity-best-practices-guideline-09132023.pdf: Central Bank of Trinidad and Tobago - Confirm whether this link is still valid.		The Authority thanks TTBS for the notice regarding the validity of the link to the *Cybersecurity Best Practices Guideline* of the Central Bank of Trinidad and Tobago (CBTT). The CBTT had updated its website and therefore the link became invalid. The References section of the Cybersecurity Framework has been revised to include the following valid link to the CBTT Cybersecurity Best Practices Guideline: https://www.central-bank.org.tt/cbtt_storage/pdf/cybe

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						rsecurity-best-practices-guideline-09132023.pdf.
21	Appendix II	Template for the Reporting of Conformance with Cybersecurity Guidelines	TTBS	Guideline 1 - Update ISO 27001	Change to TTS/ISO/IEC 27001	Changed to TTS/ISO/IEC 27001:2024.
22	4.1	Protection of Critical Network Infrastructure	Amplia	The guideline recommends adoption of ISO/IEC 27001 and implementation of zero trust architecture, but lacks specificity on timelines, metrics, and enforcement mechanisms.	• Specify minimum compliance requirements (e.g., ISO 27001 certification within 18–24 months) and require periodic third-party assessments to validate zero trust maturity.	Cybersecurity Measure 1, which is recommended, urges operators to adopt the TTS/ISO/IEC 27001:2024 standard on information security management system requirements, under the controls specified in ITU-T Recommendation X.1051. Operators who do adopt the ISO 27001 standard should submit a proposed timeframe over which the cybersecurity guidelines will be implemented. The proposed timelines will be reviewed in collaboration with the operator, as operators who are advanced in

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						their security arrangements can achieve conformance in a shorter timeframe than operators with minimal security measures in place. The measure urges operators to adopt zero-trust network architectures. This is not a requirement. However, it can be used to restrict, monitor and log management access to approved hosts and services (measure 2, point 1).
					• Map and categorize all essential network components to prioritize protection.	The following statement has been included in section 4.1: "In relation to network security, priority should be given to the infrastructure security layer, the services security layer and the applications security layer (ITU-T X.1205)."
					• Apply strict access policies and isolate sensitive systems using network segmentation.	The use of micro-segmentation of networks to minimise the breadth of potential cyberattacks

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						is referred to in the Cybersecurity Guidelines. This and strict access policies may be used to protect critical assets from internal and external threats (Measure 2, point 4).
					• Use encryption and secure protocols to protect signaling and control data.	Measure 2, point 3 addresses the need for operators to implement mechanisms to protect control channels and signalling traffic, with one such mechanism being encryption.
					• Keep firmware and software on critical systems up to date with the latest security patches.	Firmware and software on critical systems will be updated with the latest security patches during maintenance of the systems (Measure 2, point 5).
23	4.2	Network Security Monitoring and Detection	Amplia	The guidelines recommend SIEM and traffic anomaly detection but overlook integration with national threat intelligence sources (e.g., TT-CSIRT).	• Mandate integration with TT-CSIRT feeds or trusted threat intel platforms to enrich monitoring systems and improve proactive threat detection.	Through measures 19 and 20, the Authority recommends that operators securely share information on cyberattacks with other operators and incident response organisations such as TT-CSIRT. TT-CSIRT has

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
					• Implement centralized logging and real-time analytics to detect anomalies. • Establish normal traffic baselines and flag deviations for investigation. • Integrate threat intelligence to enhance detection capabilities. • Regularly audit logs and ensure retention policies meet compliance standards.	developed a framework for information sharing. Through information sharing, TT-CSIRT assists operators in detecting potential cyberattacks. This allows for centralised proactive detection and investigation of cyberattacks. This sharing of information is not currently required by law and therefore is only recommended.
24	4.3	Responsible Use and Delivery of Messaging Services	Amplia	While SMS filtering and credential transmission limitations are covered, email-based phishing and business email compromise (BEC) risks are not addressed.	• Include guidelines on secure email gateway configurations, DMARC/DKIM/SPF enforcement, and anti-phishing user training. • Filter inbound and outbound messages to block phishing and spam. • Enforce domain authentication protocols like SPF, DKIM, and DMARC to prevent spoofing.	Section 4.3 of the Cybersecurity Framework relates to the use of SMS in cyberattacks and the guidelines that may be implemented to mitigate this type of cyberattack. DMARC, DKIM and SPF are protocols specifically used to protect domain email. An operator's domain email is considered a critical asset of its network. The cybersecurity framework is generic to guide the

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						telecommunications and broadcasting industries and not specific to one type of telecommunications service. Protocols such as DMARC, DKIM and SPF, however, may be implemented in accordance with recommended Guideline 5: "Operators should protect critical assets from internal and external threats."
25	4.4	User and Network Interconnection	Amplia	The section encourages use of SBCs but stops short of defining baseline security controls for interconnection.	• Define minimum controls (e.g., mutual TLS, RPKI validation, anomaly detection at interconnection points) for all network interconnections. • Encrypt all inter-network communications using secure tunneling protocols. • Authenticate all interconnection partners and validate routing paths. • Deploy RPKI and session border controllers (BGP route filtering) to prevent unauthorized access and route hijacking.	The purpose of this framework is not to recommend specific security controls for interconnection. The cybersecurity framework is generic to guide the telecommunications and broadcasting industries. The specific security controls used to implement these guidelines will be determined by the operators/broadcasters and applied in accordance with recommended measure 12:

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						"12. Operators of public telecommunications networks and broadcasting facilities should implement appropriate security measures for user connectivity and network interconnection, to protect end users, their networks and interconnected networks."
26	4.5	Incident Response Capability and Preparation	Amplia	Guidance on incident response is useful but lacks maturity modeling and structured expectations.	• Recommend alignment with NIST SP 800-61 or ISO/IEC 27035 and require annual tabletop exercises and incident response testing. • Maintain a documented playbook for responding to cyber incidents. • Define roles, escalation paths, and communication protocols. • Conduct periodic drills and update procedures based on lessons learned.	Review, testing and updating of the cybersecurity plan are to be carried out annually. This is reflected in measure 16: "Operators should conduct annual independent testing of their networks and related systems under the plan, which can include simulations, risk assessments, vulnerability assessments, security penetration testing, governance and access control reviews, and security monitoring and detection audits."
27	4.6	Cybersecurity Plans	Amplia	The guideline assumes all operators have cybersecurity planning capacity, which may not be true for smaller entities.	• Recommend a tiered approach based on operator size and complexity; and provide a planning template with maturity levels.	It is likely that major operators would have already established cybersecurity plans and implemented measures to protect

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
					• Develop a formal cybersecurity strategy aligned with ISO/IEC 27001 principles.	their networks against cyberattacks. Networks belonging to smaller operators may not be that complicated and thus the required level of cybersecurity planning may not be as great compared to the major operators. The Authority will accept and review the cybersecurity plan or the independent certification issued by recognised relevant agencies indicating that the plan exists.
					• Include risk assessments, control objectives, and mitigation plans.	The cybersecurity plans will include risk assessments, control objectives and mitigation plans.
					• Review and revise the plan annually or after significant security events.	The guidance for the review and revision of the cybersecurity plan, annually or after significant security events, is reflected in measure 15: "15. Operators shall review this plan at least annually, or when a major threat is identified,

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						to ensure it is relevant to the threat assessment of TT-CSIRT or other recognised cybersecurity authority."
28	4.7	Reporting of Cyber Incidents	Amplia	The updated guideline adds clarity, but ambiguity remains around thresholds and timeframes for incident reporting.	• Define reporting thresholds (e.g., incidents impacting ≥100 users or involving PII breach), and require reporting within 72 hours of detection. • Establish a clear process for notifying the Authority and TT-CSIRT of incidents.	Operators would be required to submit reports only on cyberattacks, where services were either adversely affected or impaired, or user information or network elements were compromised. Full reports on cybersecurity incidents are to be submitted to the Authority within either five days of the resolution of the incident or seven days of the incident, depending on the extent of the incident (measure 18). This timeframe of five to seven days is currently adopted by the Authority. For the notification of cybersecurity incidents, operators are to notify the Authority within 12 hours of any meaningful cybersecurity incident that occurs, whether it

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						was addressed at the threat stage or involved the compromise or degradation of a network or user element and service (measure 17).
					• Use structured templates for reporting and ensure timely submission.	Operators shall report cybersecurity incidents to the Authority using the template provided in Appendix I.
					• Share anonymized threat data to support national cyber resilience.	The Authority will anonymise reports received from operators and submit the anonymised reports to TT-CSIRT. This will allow TT-CSIRT to evaluate whether its threat assessment needs to be updated and notify other operators, to ensure that their detection and protection mechanisms are in place, to mitigate ongoing cyberthreats in the industry.
29	4.8	Supply Chain and Vendor Management	Amplia	There is no defined process for risk-tiering vendors or ensuring ongoing vendor security compliance.	• Require a Third-Party Risk management Framework, including vendor classification, periodic risk reviews, and termination protocols.	Point 10, which states "establish a Third-Party Risk Management Framework, which includes vendor classification, periodic

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						risk reviews, and termination protocols. Risk reviews and vendor security assessments are to be carried out at least every three years", has been included in section 4.8.
					• Include security clauses in all vendor contracts and SLAs.	Include security clauses in all vendor contracts and service level agreements (SLAs) is covered in point 8 of section 4.8, "ensure that security hardening requirements are included in service level agreements (SLAs) with third party vendors."
					• Require third-party security assessments and compliance with ISO 27001.	Require third-party security assessments and compliance with ISO 27001 is covered in point 5 of section 4.8, "support a verification programme to ensure that vendors, particularly of critical infrastructure, follow the standards defined by the network operators and the relevant national authorities."

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
					• Monitor third-party access and conduct periodic security reviews.	Monitor third-party access and conduct periodic security reviews is covered in points 6 and 7 of section 4.8, as follows: "6. limit vendor access to only those systems for which vendors provide support". "7. ensure the integrity and security of their networks, by monitoring and logging vendor activity".
30	4.9	Subscriber Privacy and Data Protection	Amplia	The guideline restates legal provisions but misses implementation guidance for data mapping, encryption, or cross-border data transfer controls.	• Provide specific technical and governance requirements, including encryption-at-rest/in-transit, data retention limits, and DPA alignment. • Enforce data minimization and ensure lawful processing of personal data. • Use encryption at rest and in transit for personal data. • Respect data subject rights and maintain transparency in data handling.	The purpose of these guidelines is not to recommend specific security controls for the implementation of subscriber privacy and protection of data. The cybersecurity guidelines are generic to guide the telecommunications and broadcasting industries. The specific security controls used to implement these guidelines will be determined by the operators/broadcasters.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
31	4.10	Awareness, Education and Training	Amplia	The recommendation to provide "all tools necessary" may be interpreted inconsistently.	• Reframe to emphasize "all reasonable tools and resources necessary, proportionate to role and risk exposure," and require role-based training. • Provide mandatory role-based cybersecurity training. • Run awareness campaigns and phishing simulations to build resilience. • Educate customers on safe usage practices and emerging threats.	The term "all the tools necessary to fulfil their responsibilities", which is stated in the document, implies that the tools, including training, should be proportionate to the role of the employee or "their responsibilities". Role-based cybersecurity training and phishing simulations is covered by measure 23. Educating customers on safe usage practices and emerging threats is covered by measure 26.
32	4.11	Monitoring and Conformance	Amplia	The section implies public disclosure of compliance status without defining the review criteria or dispute resolution mechanisms.	• Define a standardized compliance scoring rubric and offer an appeal mechanism for disputed compliance assessments. • Conduct internal audits to assess adherence to cybersecurity guidelines.	The Template for the Reporting of Conformance with Cybersecurity Measures found in Appendix II of the document allows operators to indicate their level of compliance in relation to each measure. The Authority acknowledges Amplia's recommendation of

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
					• Maintain a compliance matrix and track progress toward full conformance.	defining a scoring rubric against which an operator's level of compliance with the guidelines would be evaluated. When these guidelines have been implemented and matured throughout the sector, the Authority may then adopt benchmarking or a scoring rubric by which an operator's level of compliance with the cybersecurity guidelines is assessed and published. The annual reports that indicate the level of conformance for each guideline allow the Authority to track the operator's progress to full conformance with the guidelines. This achieves the same intent as a compliance matrix.
33	4.1	Protection of Critical Network Infrastructure :	Michael A. Ramesar	There is no specific form of measurable compliance.	Guideline 2 should be elevated from 'recommended' to 'required' with specific technical specifications for: Multi-factor authentication for all administrative access	The Authority disagrees with the recommendation to change guideline, now measure, 2 to required, which would mandate multi-factor authentication for all

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						administrative access. The Authority recognises that the TTS/IS0/IEC 27001 standard recommends multi-factor authentication for all administrative access, and that many organisations have adopted the TTS/IS0/IEC standard within their policies. However, currently, the Authority has not identified adequate legal standing to make this required, particularly with reference to multi-factor authentication for administrative access. Currently, there is no legislation that mandates network segmentation and encryption for control channel communications to be implemented throughout the telecommunications and broadcasting sectors. Hence these guidelines are recommended and generic, to allow operators and broadcasters to determine the specific security
					Network segmentation requirements with defined security zones Mandatory encryption for control channel communications	

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						protocols they wish to implement. Micro-segmentation and encryption, however, have been mentioned in section 4.1 as possible measures to protect critical network infrastructure.
34	4.5	Incident Response Capability and Preparation	Michael A. Ramesar	The section is descriptive without specific and measurable timelines. International standards consistently require immediate notification to enable rapid coordinated response. as it is there is room for ineffective compliance. Putting in specific times leave no room for argument.	Guideline 13 requires strengthening to include: Mean Time to Detection (MTTD): Maximum 1 hour for critical incidents Mean Time to Response (MTTR): Maximum 4 hours for containment actions Customer notification: Within 72 hours when personal data is compromised or some measurable form of detection and response times	The Authority is not specifying in its guidelines mean time to detect (MTTD), mean time to respond (MTTR) or customer notification timeframes, Operators are to include these parameters in their security plans as their MTTD and MTTR may differ based on their operations.
35	4.8	Supply Chain and Vendor Management	Michael A. Ramesar	Supply Chain cyberattacks are among the top three root causes and vectors for incidents and this requirements should not be a 'recommended' but a 'required'	Guideline 21 should be upgraded to 'required' including:	The Authority disagrees with the recommendation to change guideline, now measure, 21 to required. The Authority recognises that the TTS/IS0/IEC 27002 standard recommends that vendor supply chain security

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						measures be implemented and that organisations may have adopted the TTS/IS0/IEC 27002 standard within their policies. However, the Authority currently has not identified adequate legal standing to revise this recommended measure to required.
					Annual vendor security assessments using standardized frameworks	Annual vendor security assessments have been included in point 10. With respect to how frequently vendor security assessments should be done, the Authority will allow the operator and the third-party vendor to determine how regular the assessments should be done. However, the Authority recommends that a security assessment be done at least every three years. Recently added point 10 has been amended as follows: "10 establish a third-party risk management framework, which

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						includes vendor classification, risk reviews, vendor security assessments and termination protocols. Risk reviews and vendor security assessments should be carried at least every three years."
					Contractual security requirements including incident notification obligations	Contractual security requirements, including incident notification obligations, are covered by point 8 of section 4.8: "Operators should ensure that security hardening requirements are included in service level agreements (SLAs) with third-party vendors."
					Regular penetration testing of vendor-supplied systems	Regular penetration testing of vendor-supplied systems is covered by point 3 of section 4.8: "Operators should require third parties to test and verify that all equipment, software and systems are in accordance with established security best practices."

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
36	4.11	Monitoring and Conformance	Michael A. Ramesar	There is no mention of conducting a cybersecurity risk assessment and having it updated regularly with a risk action plan.	Require annual risk assessments using standardized methodologies like NIST or ISO 27005 and implement key performance indicators for cybersecurity effectiveness. The Risk action plan should have due dates and who is accountable for closing the actions.	A risk action plan is to be included in an operator's cybersecurity plan. Section 4.6 has been revised to reflect this, accordingly. The risk action plan is to be carried out via risk assessments, and other drills. Measure 16 has been revised to include risk assessments, as follows: "16. Operators should conduct annual independent testing of their networks and related systems under the plan, which can include simulations, risk assessments, vulnerability assessments, security penetration testing, governance and access control reviews, and security monitoring and detection audits."
37	Appendix II	Template for the Reporting of Conformance with	Michael A. Ramesar	As it stands, the template's self reporting of conformance is based on 'trust' only. There needs to be a 'trust but verify' culture and mindset.	Add a section in the template to indicate and Evidence Section which can be made available to be verified and audited.	The Authority agrees with the recommendation and has added a "Compliance Verification" column to Appendix II: Template for the Reporting of

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
		Cybersecurity Guidelines				Conformance with Cybersecurity Measures.
38		Entire Document	SCF	SCF appreciates the opportunity to contribute to this consultation process and to share its perspective on the proposed cybersecurity guidelines. This response does not represent an exhaustive account of SCF´s position on the consultation. The absence of comments on any specific matter should not be interpreted as a definitive position on that issue.		The Authority thanks SCF for its feedback on the Cybersecurity Guidelines, now Framework.
39		Entire Document	SCF	We acknowledge the Authority's efforts to enhance cybersecurity within the telecommunications sector. However, SCF considers that a "one-size-fits-all" approach may not be appropriate for all operators given their distinct roles and operational scopes. As a wholesale submarine cable operator, our responsibilities and risk profile differ significantly from those of retail or mobile network operators. We believe that differentiated guidelines that reflect the distinct role of submarine cable providers in global connectivity are essential for effective and proportionate cybersecurity measures.	SCF recommends that the Authority consider developing differentiated guidelines or specific carve-outs for wholesale submarine cable operators to ensure that cybersecurity obligations are proportionate to their operational scope, risk profile, and the services they provide.	The purpose of these guidelines/measures is not to recommend specific measures for each type of telecommunications service provider. The cybersecurity guidelines are intended to be generic, to guide all operators within the telecommunications and broadcasting industries. However, if an operator thinks that a guideline/measure does not apply to its network, "not applicable" should be indicated in the column provided on the Template for the Reporting of

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						Conformance with Cybersecurity Measures. The Authority will then verify if the guideline is or is not applicable to the relevant telecommunications network or broadcasting facility.
40	4.1	Protection of Critical Network Infrastructure (Guideline 1)	SCF	We note that Guideline 1, regarding the adoption of ISO 27001, is now classified as "Recommended." However, it is important to clarify that SCF's direct operations is not covered under a separate, standalone ISO 27001 certification.	SCF supports in principle, the future alignment with ISO 27001 certification as part of a broader approach to enhancing cybersecurity practices. However, we respectfully recommend the Authority continue to classify this as "Recommended" giving the significant time and cost implications associated with implementation. We further suggest that, prior to making this guideline required, the Authority engage in further consultation with affected stakeholders to evaluate the considerations raised (timelines and associated costs).	The intention is not to make the adoption of TTS/ISO/IEC 27001 a requirement for telecommunications operators and broadcasters, as the Authority has not identified any country that has mandated ISO/IEC 27001 compliance on its telecommunications operators. The Authority agrees that there would be a significant cost to operators, particularly the smaller operators, to mandate adoption and implement the TTS/ISO/IEC 27001 standard.
41	4.1	Protection of Critical Network	SCF	We agree with the importance of the capabilities outlined for protecting critical network infrastructure. However, specific definitions are needed for terms such as "critical events" and "critical core network elements"	We recommend that the Authority define a baseline set of "critical events" and "critical core network elements" relevant to submarine cable	The guidelines/measures are intended to be generic and, as a result, the definition of a critical network infrastructure adopted

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
		Infrastructure (Guideline 2)		in the context of submarine cable systems to ensure appropriate application. The obligation to maintain equipment at their most secure versions should also consider the operational constraints of submarine systems, where immediate remediation may not always be feasible.	operations, allowing operators to customize based on risk assessments and asset criticality. We also recommend that the obligation to maintain equipment at secure versions considers operational constraints of submarine systems, allowing for alternative security measures when immediate remediation is not feasible.	by the Authority in the document is generic to any type of telecommunications network or service, rather than individual types of core services. The Authority does note that elements such as the optical fibres, protective layers, repeater/amplifiers and land-based components are critical to submarine cable networks, and that data interception, and tampering and signal interference are the types of cyberattacks that affect subsea cable operations. However, with the guidelines being generic, these elements and events will not be included in the guidelines but are instead referred to as core equipment and incidents throughout the document.
42	4.1	Protection of Critical Network Infrastructure	SCF	SCF operates both private and public IP-based networks: one for internal management of transmission networks and one for SCF customers. Therefore, the	We acknowledge the applicability of this guideline to SCF's IP networks and will continue to deploy secure and resilient DNS infrastructure	The Authority commends and encourages SCF to continue deploying secure and resilient

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
		(Guideline 4.3)		guideline to deploy secure and resilient DNS infrastructure is applicable to SCF's IP networks.	according to industry-recognized standards.	DNS infrastructure according to industry-recognised standards.
43	4.2	Network Security Monitoring and Detection (Guidelines 4, 5, 6, 7, 8, 9)	SCF	We acknowledge the importance of network security monitoring and detection. SCF considers that there are no technical limitations on monitoring traffic in a submarine cable, provided the right monitoring and supervision tools are used. We also agree that robust cybersecurity monitoring and protections are essential to safeguard internal corporate networks and ensure service availability and integrity. However, it is crucial to distinguish between an operator's responsibility for their network and a customer's responsibility for their own internal data networks and internet usage.	We agree with the stated guidelines for network security monitoring and detection and confirm our ability to implement them for submarine cable traffic. We recommend clarification that while operators are responsible for safeguarding their networks and preventing threats emanating from them, customers are responsible for implementing cybersecurity measures within their own internal "data" networks and for their activities on the internet.	The Authority agrees with SCF's recommendation and has included the following statement in section 4.4, "User and Network Interconnection": "End users or customers are responsible for implementing cybersecurity measures within their own data networks that are beyond the network demarcation point."
44	4.3	Responsible Use and Delivery of Messaging Services (Guideline 10)	SCF	SCF agrees with the importance of conducting regular cybersecurity risk assessments and vulnerability scanning to identify and mitigate threats. However, the frequency of "regular" needs to be clearly defined, and the scope of these assessments for submarine cable infrastructure should be proportionate to the specific risks and operational environment of wholesale providers.	We recommend that the Authority provide clear guidance on the appropriate frequency and scope of cybersecurity risk assessments and vulnerability scanning for submarine cable operators, aligning with international best practices for critical infrastructure. The focus should be on the unique risks associated with undersea cables and associated landing stations, rather than general network operations.	Guideline, now measure, 18 indicates that risk assessments should be carried out annually by all operators. The cybersecurity guidelines are intended to be generic to guide all operators within the telecommunications industry, no matter their core business. Therefore, no scope of cybersecurity risk assessments and vulnerability scanning in relation to a particular type of

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						service is included in the guidelines. SCF, however, are encouraged to carry out their risk assessment and vulnerability assessment processes in alignment with international best practices.
45	4.3	Responsible Use and Delivery of Messaging Services (Guideline 11)	SCF	We agree with the principle of managing cybersecurity risks and implementing controls to protect critical assets. This includes measures such as encryption, access controls, and network segmentation. For submarine cable systems, the critical assets are primarily the physical cable, the optical transmission equipment, and the landing station infrastructure. The implementation of controls should be proportionate to the identified risks and the nature of the wholesale services provided.	We recommend that the Authority emphasize a risk-based approach to implementing cybersecurity controls, allowing operators to prioritize measures that address the most significant threats to their specific critical assets. Guidelines should be flexible enough to accommodate the specialized nature of submarine cable operations and the controls already in place due to international standards and consortium agreements.	The Authority agrees that a risk-based approach to implementing cybersecurity controls for the protection of critical assets should be done by the operators. This risk-based approach, which would be conducted through risk assessment, would be conducted annually, as recommended in Guideline, now measure, 18. The cybersecurity guidelines are generic to guide all operators within the telecommunications industry and are flexible enough to accommodate the specialised nature of submarine cable operations and the control protocols already in place.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
46	4.4	User and Network Interconnection (Guideline 12)	SCF	We agree on the importance of protecting interconnection points like cable landing stations. However, submarine cable operators, including SCF, do not provide user connectivity as we primarily serve network service providers. Therefore, the aspect of the guideline pertaining to "user connectivity" does not directly apply to our operations. Regarding customer premise equipment (CPE), operators should only be responsible for equipment they own or manage	We recommend clarifying that operators are responsible for securing their own network and the interfaces they control, but not the security of external networks they interconnect with. Specifically, for submarine cable operators, the guideline should focus on network interconnection points, not user connectivity. We also recommend adjusting the statement "Operators should also ensure that customer premise equipment is maintained securely through appropriate patching and upgrades" to "Operators should also ensure that customer premise equipment, that are owned or managed by the operator, is maintained securely through appropriate patching and upgrades."	The Authority agrees with SCF that only the network interconnection aspect of Guideline, now measure, 12 applies to submarine cables, and not user connectivity. The Authority agrees with SCF and has made the following revision in section 4.4: "Operators should also ensure that customer premise equipment that is owned or managed by the operator is maintained securely through appropriate patching and upgrades."
47	4.5	Incident Report Capability and Preparation (Guideline 13)	SCF	We understand the importance of incident response plans as a part of national cybersecurity measures and agree that all operators should have documented response capability. However, the current guideline assumes a "one-size-fits-all" approach. Submarine cable operators typically do not serve individual customers but rather other telecom providers and network partners. Therefore, the requirement to notify	We recommend adjusting this guideline to reflect the specific role of submarine cable operators in the communications network, ensuring that monitoring and response expectations match their specific risks. Any requirement to notify "customers" should instead refer to	The term "customers", as used in in Guideline 13, also refers to "relevant partners or service providers who depend on subsea cables". SCF is asked to note that the reporting of cybersecurity

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				"customers" needs to be rephrased for our context. We previously highlighted that the definition of "incident" was excessively broad, and while the latest version offers more clarity, further revision is needed to avoid ambiguity.	relevant partners or service providers who depend on the cable system. We propose a revised definition for "incident": "Operators must promptly notify the Authority of any cybersecurity incident that has, or is reasonably likely to have, a material impact on their networks, services, or subscribers' information. A material impact refers to significant disruption to service availability or quality; unauthorized access to or compromise of subscriber or operational data; incidents requiring notification to other regulatory or law enforcement bodies; or reputational or financial harm that could significantly affect customer trust or operational continuity. Incidents that are fully contained and resolved without any actual compromise, disruption, or risk of harm to users or services are not required to be reported."	incidents is dealt with in section 4.7 of the Cybersecurity Framework, and not section 4.5. The Authority disagrees with redefining "incident", as used in SCF's recommendation. The definition of incident stated in section 1.9 captures whether the attack was attempted or infiltrated, which components of the network were attacked, and the effects of the attack. For the notification of cybersecurity incidents, Guideline, now measure, 17 was revised so that operators are to notify the Authority within 12 hours of any meaningful cybersecurity incidents that occur.
48	4.6	Development and Maintenance	SCF	We agree with the importance of developing and maintaining a cybersecurity plan. However, as a wholesale submarine cable operator with limited	We request that the Authority provide clear and proportionate guidance on what such a plan should include for	An operator's cybersecurity plan comprises specific measures that will be implemented to ensure

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
		of Cybersecurity Plans (Guidelines 14, 15, 16)		operational scope, our exposure and risk profile differ from retail or mobile network operators. A one-size-fits-all approach could impose unnecessary burdens. We also support the requirement for periodic testing but believe annual independent testing would impose a significant and disproportionate financial burden on infrastructure-based operators with limited attack surfaces.	different categories of operators. We are open to working with the Authority to develop a fit-for-purpose plan. We recommend a risk-based, flexible approach to independent testing that allows operators to tailor the frequency, scope, and method of testing to their operational model, perhaps allowing for rotation of testing domains over a 2–3-year cycle or leveraging vendor security assessments.	that their network is secure from cyberattacks. Each operator will develop a plan that is relevant to their specific network or facility. The Authority disagrees with SCF's recommendation for the rotation of testing domains over a two to three-year cycle. The Authority deems cyberattacks to be an ever-increasing risk to telecommunications networks and urges operators to conduct tests annually, which should include risk assessments and vulnerability assessments.
49	4.7	Reporting of Cyber Incidents (Guidelines 17, 18, 19, 20)	SCF	We agree with the need to report significant cybersecurity incidents but believe mandatory reporting should apply only to incidents that cause actual degradation of critical services or compromise sensitive information. Reporting "any unusual threat" without impact could result in excessive administrative work. The proposed 5-day and 7-day deadlines may also be challenging for smaller operators. As a wholesale provider, the requirement for a "customer notification plan" does not apply to SCF as we do not serve end users directly. While we support reporting to appropriate national authorities and incident response organizations with secure handling of information, we	We request that the Authority introduce tiered reporting thresholds and timelines that reflect the operator's size and role. Only "incidents" that cause significant harm to services, users, or network elements should be reported. The "customer notification plan" requirement should be clarified to apply only to operators serving end users directly. We strongly recommend that any sharing of	SCF is asked to note that only "incidents" that were infiltrated and caused significant harm to services, user information or network elements require full reports to be submitted. Currently, the Authority has not established a tiered approach to regulating telecommunications operators. Therefore, the reporting threshold and

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				do not support the recommendation to share incident information with other operators due to confidentiality concerns, commercial sensitivities, and operational irrelevance for submarine cable operations.	incident information with other operators be voluntary, based on mutual agreements or formal frameworks, and not imposed as a general obligation.	timeframes established in the guidelines apply to all operators. The Authority does not agree that the "customer notification plan" requirement should be applied only to operators serving end users directly. Operators of subsea cables will require a customer notification plan during instances when service to their customers (connected terrestrial operators) is affected due to cyberattacks on their subsea infrastructure. In terms of the guidelines, now measures, related to secure information sharing between operators, these are only recommended. Operators are encouraged to share information with other operators based on mutual agreements and at their discretion. The sharing of cybersecurity information is a best practice observed in other

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						jurisdictions such as Canada and Europe.
50	4.8	Supply Chain and Vendor Management (Guideline 21)	SCF	We agree on the importance of cybersecurity risks in supply chain and vendor relationships. However, submarine cable operators often work with international vendors, which limits our ability to control vendor selection or apply local security requirements directly. Vendors may also operate under different regulatory regimes.	We recommend that this guideline be flexible, taking into account whether the operator has direct control over the vendor or equipment, the international nature of submarine cable systems, and existing industry or international standards already in place.	The Authority acknowledges that submarine cable operators may not have direct control over the vendor or equipment operators. However, submarine cable operators are expected to implement control mechanisms in relation to their supply chain agreements, where they can.
51	4.9	Subscriber Privacy and Data Protection (Guideline 22)	SCF	We agree with the importance of protecting subscriber privacy rights.	We agree with this guideline.	The Authorities notes SCF's agreement regarding Guideline, now measure, 22.
52	4.10	Cybersecurity Awareness, Education and Training (Guidelines 23, 24, 25, 26)	SCF	We support the principle of appropriate cybersecurity awareness and training for staff. However, as a submarine cable operator with a small, specialized workforce, training requirements should be proportionate to our operational scope and staff size. Our staff already receive specialized training through industry programs and vendor certifications. Regarding customer information (Guideline 26), submarine cable operators do not provide services directly to end users, so requirements for customer	We recommend that the Authority recognize existing industry-specific training programs rather than requiring duplicative general telecommunications cybersecurity training, and that training requirements be scaled appropriately for smaller, specialized operators, allowing credit for existing industry certifications. Obligations regarding	The Authority does not require operators to undergo duplicative general telecommunications cybersecurity training. Guideline, now measure, 23 recommends that members of staff undergo appropriate cybersecurity training relevant to their field of work within the telecommunications sector. Like

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				cybersecurity education do not apply to our wholesale operations. The phrasing "all the tools necessary" in Guideline 25 is overly broad and impractical, potentially implying an unbounded obligation.	customer cybersecurity education (Guideline 26) should focus on our relationships with licensed telecommunications operators who are our actual customers, rather than end users. We suggest editing Guideline 25 to: "Staff should be provided with appropriate tools and resources, proportionate to their roles, to effectively support the implementation of the company's cybersecurity protocols and standards."	end users, telecommunications operators who are customers of subsea cable operators should be educated on cybersecurity incidents associated with subsea cable networks. The Authority believes that Guideline, now measure, 25, "Staff should be provided with all the tools necessary to fulfil their responsibilities while applying the company's cybersecurity protocols", is appropriate, as it requires the "appropriate" or necessary tools to efficiently perform the roles of the staff whilst practising the cybersecurity protocols.
53	4.11	Monitoring and Compliance (Guideline 27)	SCF	Given the unique nature of submarine cable infrastructure, clarification is needed on the applicability of specific cybersecurity guidelines to this sector. We also question the legality of deeming a failure to comply with a policy guideline as a breach of concession, as policy guidelines do not hold the same legally binding effect as legislation.	We request that the Authority clarify the applicability of specific cybersecurity guidelines to the submarine cable sector. We also encourage the development of a standardized conformance reporting template and the adoption of a risk-based maturity model. We	SCF is asked to note that the purpose of this Framework is not to recommend specific measures for each type of telecommunications service provider, such as wholesale submarine cable operators. The cybersecurity framework is

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
					recommend that any non-conformance be addressed through a structured remediation process prior to any formal enforcement actions, and that conformance reports be treated as strictly confidential. We respectfully request clarification on the legal basis under which failure to comply with cybersecurity guidelines or failure to submit an annual conformance report may be deemed a breach of concession, asking whether these obligations will be reflected as explicit conditions within the concession instrument or incorporated via binding regulation.	intended to be generic, to guide all operators within the telecommunications industry, no matter their core business. The Authority clarifies that, in general, the required guidelines/ measures relate to requests for information, e.g., requests for cybersecurity plans, requests for information about incidents, and compliance reports. Accordingly, failure of the concessionaire to reply to such requests for information can give rise to a breach of concession condition A28, which sets out the requirement to furnish to the Authority requested information. The legal basis for the required guidelines is also premised on concession conditions B7 and B10 which obligate concessionaires to make certain information available and notify the Authority with respect to their networks.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						Appendix II: Template for the Reporting of Compliance with Cybersecurity Measures is to be used by operators to indicate their level of conformance with the individual guidelines. An operator partially compliant or non-compliant with a guideline will be addressed by the Authority on a case-by-case basis. An operator's Template for the Reporting of Compliance with Cybersecurity Measures will not be made public; however, a summary indicating an operator's level of cybersecurity compliance may be available publicly, for the interest and protection of consumers.
54		Entire Document	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		The Authority thanks Digicel for its feedback on the Cybersecurity Guidelines now Framework.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				response does not in any way indicate acceptance, agreement or relinquishing of Digicel's rights.		
55	4.2	Network Security Monitoring and Detection "Operators of public telecommunications networks and broadcasting facilities should be able to monitor all network traffic, whether management, control or data, to detect malicious behaviours and activity."	Digicel	Digicel agrees with this statement to the extent that it justifies why Digicel has made significant investment in robust cybersecurity monitoring and protections to safeguard it's internal corporate network and to ensure the availability and integrity of services that it provides to customers. For example, appropriate security monitoring and protections are implemented to prevent malware, DDoS and other threats that may affect the availability of our services to customers. Digicel also establishes safeguards that prevent threats within our internal network and such that could emanate/propagate from our network to affect our customer's corporate network. However, it remains the customer's responsibility to likewise implement their own cybersecurity measures to safeguard their internal "data" network. This obligation cannot fall on the operators. Digicel finds it important to distinguish this given that the provision of some services like DIA – Direct Internet Access, allows a customer the ability access the internet. The customer, however, is responsible for what they do on the internet. For example, not illegally accessing pirated content or avoiding malicious websites that can lead to malware infection of their devices. Digicel is not in a position to monitor, protect and/or safeguard a customer from intentional/unintentional acts while navigating the	TATT should also consider risks/impacts arising from the inability of customers to safeguard their internal data networks or knowingly engaging in malicious behaviour or activity.	Guideline, now measure, 26 recommends that operators of public telecommunications networks and broadcasting facilities inform their customers on how to securely use their services. This would address customers having the ability to safeguard their internal data networks.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				internet from their owned- systems or users. Digicel is not in a position to take liability or adopt measures that remains the customer's responsibility.		
56	4.4	User and Network Interconnection "Operators should also ensure that customer premise equipment is maintained securely through appropriate patching and upgrades"	Digicel	We agree with the statement to the extent that operators should ensure appropriate security setup for SIP services, such as SBCs on the portion of the network that falls within their operational scope.	Digicel recommends the statement "Operators should also ensure that customer premise equipment is maintained securely through appropriate patching and upgrades" is adjusted as follows "Operators should also ensure that customer premise equipment, that are owned or managed by the operator, is maintained securely through appropriate patching and upgrades". This would clarify that customers must patch and upgrade their owned systems since TATT agrees that customers are responsible for their own equipment.	The Authority agrees that customers must patch and upgrade their own systems and has revised the relevant statement, as follows: "Operators should also ensure that customer premise equipment that is owned or managed by the operator is maintained securely through appropriate patching and upgrades." The Authority has also included the following statement in section 4.4: "End users or customers are responsible for implementing cybersecurity measures within their own data networks that are beyond the network demarcation point."
57	4.5	Incident Report	Digicel	Digicel is not of the view that the definition and scope provided by the Authority is satisfactory and holds the view that it still requires clarification. The specific	The Authority is asked to define "incident" and "unusual attempts" to provide justifications or specified	Digicel is asked to note that the guidelines/measures relating to

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
		Capability and Preparation		parameters are not defined and thus an onerous and unmanageable obligation remains with the operators. For example, what is considered "unusual attempts". The business experiences thousands of these types of matters with no actual impact to the business or the customer due to our responses and mitigation protocols. It is unrealistic that operators be expected to report on incidents that are "unusual" as this will create endless, unrealistic and unnecessary reporting regimes.	scenarios for implementing such restrictive measures. In this vein, Digicel proposes the following amendment in order to avoid misunderstanding and ambiguity :- "Operators must promptly notify the Authority of any cybersecurity incident that has, or is reasonably likely to have, a material impact on their networks, services, or subscribers' information. A material impact refers to significant disruption to service availability or quality; unauthorized access to or compromise of subscriber or operational data; incidents requiring notification to other regulatory or law enforcement bodies; or reputational or financial harm that could significantly affect customer trust or operational continuity. Incidents that are fully contained and resolved without any actual compromise, disruption, or risk of harm to users or services are not required to be reported."	notifying and reporting cybersecurity incidents to the Authority are dealt with in section 4.7 of the Cybersecurity Framework and not section 4.5. The definition of incident stated in section 1.9 is as follows: "Incident: an event having a potential or actual adverse effect on the security of a public telecommunications network (ENISA 2021) or broadcasting facilities, and comprising an attempt to infiltrate, or actual infiltration of, a network element or system, or the degradation or loss of public telecommunications service due to a cyber threat or cyberattack." For the notification of cybersecurity incidents, Guideline, now measure, 17 now states:

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						"17. Operators of public telecommunications networks and broadcasting facilities shall notify the Authority within 12 hours of any meaningful cybersecurity incident that occurs, whether the incident was unusual and addressed at the threat stage or involved the compromise or degradation of a network or user element and service, or user information." For the reporting of an incident, Guideline, now measure, 18 now states: "18. For cybersecurity incidents where telecommunications networks or broadcasting facilities were compromised and services were adversely affected or impaired, operators shall submit an incident report to the Authority no later than five days after resolution where the incident is resolved within five

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						days or, for incidents not resolved within five days, within seven days of the start of the incident, specifying the nature of the incident, the services affected, the scope of the impact of the incident, their customer notification plan, the timeframe for resolution of the incident, and any other matter the Authority may reasonably require."
58	4.6	Development and Maintenance of Cybersecurity Plans References to threat assessment of TT-CSIRT	Digicel	We acknowledge the feedback that independent certification which verifies the existence of a CIRP is adequate. ISO 27001 certification is independent and validates the existence of a CIRP. Digicel Caribbean is certified ISO 27001 compliant and this would cover Digicel Trinidad and Tobago since the market complies with Group-wide policies and obtains cybersecurity operations and incident response from the central security team. However, would operators be required to submit sensitive and confidential aspects of their cybersecurity architecture to the Authority?	The Authority is asked to clarify and outline the necessary and robust cybersecurity protocols that they have in place to protect sensitive and confidential data that may be shared by an Operator to the Authority. Digicel nor the Authority would want to create a situation where the operators are trying to quell and mitigate a breach or cyber-attack, and then have such information further shared with the Authority and made further susceptible to leaks, attacks and cybersecurity risks.	The Authority asks Digicel to note that the Authority treats with confidentiality all information submitted by operators in relation to the development of their networks. Guideline/measure 14, however, permits operators to submit suitable, independent certification of the existence of their cybersecurity plan, where applicable, instead of submitting or sharing any confidential or proprietary information. The Authority has its own cybersecurity protocol in place

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						for the protection of confidential information submitted by concessionaires.
59	4.7	Reporting of Cyber Incidents	Digicel	Are there any provisions that restrict other network operators from publishing/sharing and or leaking the identity of the affected operator? This is to minimize as much as possible any loss of consumer goodwill/brand reputation and give the affected operator the latitude to robustly treat with the cybersecurity incident and not spend resources on damage limitation and litigating the incident in the public domain.	The Authority is asked to provide clear definitions, classifications, and scenarios for what constitutes an "incident."	The variety of services provided by telecommunications operators is broad and, with 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. The sharing of cybersecurity information between operators is only a recommended guideline (Guideline, now measure, 19). However, if operators do decide to share cybersecurity information between themselves, mutual agreements may be established, to restrict the publishing/sharing of confidential information that may affect any operator.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				Further, Digicel is not in agreement that non- routine incidents that do pose risk to services be reported as this is an onerous and unmanageable reporting request. Further incidents that do not pose a risk will not have impact to the customer base, therefore, should not be deemed as necessary to report. In relation to Guideline 19, Digicel continues to outright rejects any sharing of information with other operators as this would have major confidential and commercial risks to our operations.	Further, Digicel maintains and 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. Digicel requests that the circumstances under which reports are given, whether by timeline or voluntarily be specifically defined and only ones that are considered and defined as material to the business and topic of cyber security incidents. The definition of incidents and parameters under which same are reported are yet to be satisfactorily itemised/defined by the Authority.	The Authority agrees with Digicel's recommendation that only incidents that cause significant harm to services, users or network elements should be reported. The Authority should be notified of non-routine incidents that do pose a risk to services. For the notification of cybersecurity incidents, operators are to notify the Authority within 12 hours of meaningful cybersecurity incidents that occur, whether it was addressed at the threat stage or involved the compromise or degradation of a network or user element and service. For the reporting of an incident, operators shall submit to the Authority, within five after resolution or seven days of the incident, depending on the extent

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						of the incident, an incident report comprising the nature of the incident, the services affected, the scope of the impact of the incident, their customer notification plan, the timeframe for resolution of the incident, and any other matter the Authority may reasonably require.
60	4.10	Cybersecurity Awareness, Education and Training	Digicel	Digicel is of the view that providing 'every possible tool' to every staff member is overly far reaching.	Digicel suggests the following amendment be made in order to maintain the intent of enabling staff to uphold cybersecurity standards, while not implying an unbounded obligation that disregards the commercial constraints of the business:- "Staff should be provided with appropriate tools and resources, proportionate to their roles, to effectively support the implementation of the company's cybersecurity protocols and standards."	The term "all the tools necessary" does not imply "every possible tool". Necessary tools mean the tools that will allow staff to carry out their work while implementing company cybersecurity guidelines. This does not imply that every possible tool shall be purchased, just the tools required.
61	4.11	Monitoring and Compliance	Digicel	Digicel is of the view that the Authority has confused /failed to differentiate the concept and legality of the Concession, legislation or regulations ("laws") as the case may be, and policy guideline created by		The Authority clarifies that the document provides both recommendations and requirements. The requirements

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
		"…Failure to submit the annual conformance report or comply with a required guideline may be deemed as a breach of concession and the Authority shall act as prescribed under the concession or the Act."		guidelines or policies the Authority. The legally binding effect of laws cannot be given the same weight as a guideline created by the Authority. While we acknowledge that the guidelines are guided by the laws, this does not automatically equate to the policy guidelines carrying the same legal effect. There is also the question of whether the policy guideline truly reflects the intention of the laws and whether this guideline is even contemplated the purpose of section of the law it relies upon. The Authority can further ask itself, can a court action be brought or based on policy guideline or only through a breach of a Concession, Act or Regulation. Respectfully, Digicel maintains the view that a failure to comply with a policy guideline cannot constitute a legal breach of the Concession, Act or Regulation.		are based on specific concession conditions, in particular, A28, B7 and B10 which obligate concessionaires to notify, provide or make information available to the Authority upon request. The document presents guidance to the relevant concessionaires on what information the Authority will be requesting as it relates to cybersecurity. Failure to respond to the request by the Authority, made in accordance with the concession condition, can result in a breach of the concession. The Authority has amended the document to more clearly identify the specific regulatory obligations. These amendments consist of the revision of section 1.5 of the document to include sections 18 (1) (a) (g) (h) and (m) of the Act:

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						"Subject to the provisions of this Act, the Authority may exercise such functions and powers as are imposed on it by this Act and in particular – a) make recommendations to the Minister on the granting of concessions and licences and g) ensure compliance with the Convention; h) implement and enforce the provisions of this Act and the policies and Regulations made hereunder; m) investigate complaints by users, operators of telecommunications networks, providers of telecommunications and broadcasting

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						services or other persons arising out of the operation of a public telecommunications network, or the provision of a telecommunications service or broadcasting service, in respect of rates, billings and services provided generally and to facilitate relief where necessary;" Also now included in section 1.5 are sections A28, B7, B8, B9 and B10 of the Concession Agreement for the Operation of a Public Telecommunications Network and/or Provision of Public Telecommunications and/or Broadcasting Services, as follows:

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						A28. The concessionaire shall furnish to the Authority, in such manner and at such times as the Authority may reasonably direct, either in writing or by a general notice published by the Authority, such information related to the activities of the concessionaire under this Concession, including but not limited to network or service development plans, financial, technical and statistical information, accounts, service performance metrics and other records, as the Authority may reasonably require in order to perform its functions. B7. The concessionaire shall make such information

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						available, promptly and without charge, to the Authority or to any person or entity authorised by the Authority for inspection and shall provide copies of the information as required (in such format as the Authority may reasonably require) for the Authority's purposes. B8. The concessionaire shall, at the request of any other holder of a concession granted under the Act and without unnecessary delay, give reasonable access to such information for the facilitation of network planning, maintenance, and reconfiguration. The concessionaire shall be entitled to charge a reasonable fee to recover

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						costs it incurs in connection with the provision of such information to other concessionaires. B9. The concessionaire shall notify the Authority of any proposed material changes to the Public Telecommunications Networks forthwith and provide to the Authority such information as the Authority shall reasonably require for the purpose of assessing the effect of such changes, prior to effecting the changes. B10. The concessionaire shall not, without the prior written approval of the Authority, such

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						approval not to be unreasonably withheld, make any changes to the Public Telecommunications Networks which might reasonably be anticipated to have a material adverse technical effect on any telecommunications network or service or broadcasting service or any consumer of any telecommunications network or service or broadcasting service provided by the concessionaire or any other person or entity.
62		General	CCTL	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 Columbus Communications Trinidad Limited's (CCTL's) rights.		The Authority thanks CCTL for its feedback on the Cybersecurity Guidelines/Framework.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				CCTL would like to reiterate its gratitude to the Telecommunications Authority of Trinidad and Tobago ("TATT", "the Authority") for its initiative in addressing cybersecurity for public telecommunications networks and broadcast facilities and welcomes the opportunity to comment on these proposed Guidelines. CCTL still believes that the Guidelines are a noteworthy attempt at ensuring that cybersecurity practices are strategically contextualised and furthermore embedded into the operations of providers of public telecommunications networks and broadcasting facilities.		
63	1	Introduction	CCTL	As regards the Authority's comments in the Addendum to Decisions on Recommendations of the First of Two Rounds for these Guidelines ('the Addendum"), CCTL acknowledges the Authority's reference to existing sections. However, these sections describe a desired end-state without addressing the fundamental "governance gaps" CCTL highlighted. The core issue remains that the Guidelines impose obligations that are not clearly anchored in law		The Authority clarifies that the document provides both recommendations as well as requirements. The requirements are based on specific concession conditions, in particular, A28, B7 and B10 which obligate concessionaires to notify, provide or make information available to the Authority upon request. The document presents

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				specific to cybersecurity. Simply stating that the notation is not new does not resolve the unfortunate confusion it creates when applied to a sensitive and dynamic field like cybersecurity, where a clear legal and governance framework is paramount. According to the Trinidad and Tobago Gazette Vol. 64 No. 81 of Friday 23 May, 2025, authority has been assigned to the Ministry of Homeland Security to champion such legislative and policy framework. Documents prioritised by the Trinidad and Tobago Computer Security Incident Reporting Team (TT-CSIRT) highlight the very gaps that were previously raised as some are in draft, not fully proclaimed, or outdated. CCTL acknowledges that the Authority may have sought guidance for applicable practices from jurisdictions that have advanced legislative frameworks for cybersecurity. However, the Authority may have fallen short in creolising such proposals in reconciling desired-state behaviours with Trinidad and Tobago's extant legislative and policy framework to ensure relevance of actions. Guidelines are expected to reduce ambiguity that may arise within legal framework. CCTL maintains that without this clarity, the Guidelines risk being		guidance to the relevant concessionaires on what information the Authority will be requesting as it relates to cybersecurity. Failure to respond to the particular requests by the Authority, made in accordance with the concession conditions can result in a breach of the concession. The Authority has amended the document to more clearly identify the specific regulatory obligations. These amendments consist of the revision of section 1.5 of the document to include sections 18 (1) (a) (g) (h) and (m) of the Act and sections A28, B7, B8, B9 and B10 of the Concession Agreement for the Operation of a Public Telecommunications Network and/or Provision of Public Telecommunications and/or Broadcasting Services.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				incongruous to TATT's mandate of consumer protection, let alone national cybersecurity objectives.		
64	1.5	Relevant Legislation	CCTL	In the Addendum, CCTL notes TATT's response to the appropriateness of the proposed approach and contends that attention be paid to the nuances of same, having regard to complementarity as fostered in the Central Bank of Trinidad and Tobago's (CBTT) guidance for the financial sector, versus required actions that are not rooted in extant legal framework. It should be noted that the financial sector does have more advanced legislation to address risks, which make CBTT's guidance adequate to its regulated entities. Specifically, CCTL believes that despite their good intentions, the exact language of Guidelines 13, 14, 15, 17, 18, 22 and 27 is more relevant to legislative instruments. CCTL seeks clarification as to whether TATT intended to create regulation on these matters as opposed to Guidelines given the inference of concessionary repercussions for non-compliance. As the Authority may be aware, there are indeed similar mandates in other jurisdictions to secure networks and file items such as System Security and Integrity (SSI) Plans with the United States Federal	CCTL recommends that the Authority addresses the requisite legislative gaps within its purview, and champion related laws, to bring meaningful effect to cybersecurity objectives from a telecommunications sector perspective.	The Authority clarifies that there was no intention to create regulations. The requirements are based on specific concession conditions, in particular A28, B7 and B10 which obligate concessionaires to notify, provide or make information available to the Authority upon request. The document presents guidance to the relevant concessionaires on what specific information the Authority will be requesting as it relates to cybersecurity. Failure to respond to the particular requests by the Authority, made in accordance with the concession conditions, can result in a breach of the concession. The Authority has amended the document to more clearly identify the specific regulatory

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				Communications Commission (FCC) (S102 of the Communications Assistance to Law Enforcement Act (CALEA)), and Canada's Critical Cyber Systems Protection Act (CCSPA). CCSPA empowers the government to require telecommunications service providers to, inter alia: • implement security measures including vulnerability assessments; • develop and maintain cybersecurity plans; • report cybersecurity incidents; and • remove specific products from networks if deemed high-risk In these examples, there have been clear steps to designate operators of critical cyber systems and facilitate much needed cybersecurity cooperation where clear procedural rules are key to effective action. While CCTL operates in full compliance with the Act and its concession, CCTL reiterates that these instruments were not designed to manage the intricacies of national cybersecurity. CCTL's concern is that the Guidelines attempt to address broad cybersecurity issues, such as those covered by the still-pending full proclamation of the Data Protection Act 2011 and the dated Computer Misuse Act 2000,		obligations. These amendments consist of the revision of section 1.5 of the document to include sections 18 (1) (a) (g) (h) and (m) of the Act and sections A28, B7, B8, B9 and B10 of the Concession Agreement for the Operation of a Public Telecommunications Network and/or Provision of Public Telecommunications and/or Broadcasting Services. The Authority disagrees that legal ambiguity has been created. To be clear, the provisions contained in these Guidelines/ Framework are to be construed

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				through general clauses in the Telecommunications Act. This creates legal ambiguity. For example, an operator's ability to protect customer information is indeed linked to Quality of Service (QoS), but this does not automatically grant the Authority the purview to approve detailed, highly sensitive network security plans, a point CCTL addresses further on in these comments.		and interpreted in accordance with the laws of Trinidad and Tobago, and more specifically, the Act. Further, the Authority has supported, and continues to support, its line Ministry and other relevant agencies in the much-needed updating of the relevant ICT-related legislation. The Authority reiterates its objective to assist operators in protecting the public telecommunications networks from unauthorised access, misuse and theft and, in so doing, protect consumers who use these networks and their data, in accordance with its statutory mandate of consumer protection.
65	4	Guidelines for Cybersecurity of Public Telecommunications	CCTL	Guideline 1: Adoption of international standard ISO 27001 under the controls specified in ITU-T Recommendation X.1051. This risk-based approach is practical and respects the varying capabilities and resources of operators.	CCTL proposes that a predictable framework be established beforehand, clearly defining what constitutes public-facing information (e.g. certification status) versus confidential security practices that	CCTL is asked to note that operators may submit to the Authority their cybersecurity plan or "suitable independent certification of the existence of their cybersecurity plan".

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
		Networks and Broadcasting Facilities		However, the decision to assess the confidentiality of security practices on an individual basis is concerning. This approach introduces significant regulatory uncertainty and is inefficient for both the Authority and operators.	underpin the very effectiveness of our defences.	These plans shall detail the specific measures that operators will implement to ensure their networks and corresponding elements are secure; critical network infrastructure is hardened and protected as far as reasonably possible; how the security of the network and threats, attacks and compromises will be monitored and logged; how operators will respond to incidents, whether purely at the threat stage or if an actual cyberattack has occurred; and how the security of the network will be continually tested and updated, including details of a risk action process. The Authority will treat an operator's cybersecurity plan with confidentiality. However, the level of compliance with the guidelines to which an operator is

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						adhering will be made public, in the interest of the consumer.
66	4.5	Incident response capability and preparation	CCTL	Guideline 13: Incident Response Capability and Preparation In response to Item 6 of the Addendum, CCTL strongly contests this position. While CCTL agrees that security impacts QoS, the Authority's assertion that a "network security plan" is analogous to a "network development plan" under Section 24(1)(a) of the Act is a significant overreach of regulatory scope. As S24 (1)(a) was not drafted with the intricacies of enhanced cybersecurity cooperation in mind, CCTL reiterates that loose interpretation of this section will continue to foster uncertainty. S24 (1)(a) is procedurally limited as it provides insufficient, proportionate details on consequences for inadequate incident response capabilities, and standards for determining adequacy. TATT's approach does not provide guidance for material losses, mitigating risks to critical sectors underpinned by communications, and clear procedural rules for cooperation as anticipated in jurisdictions where	CCTL maintains that this Guideline be reconstructed as a voluntary mechanism to encourage the development of incident response capability and preparation, and facilitate requisite dialogue on common threats, cognisant of the disparate capabilities of operators, confidentiality matters and extant legislative gaps to ensure certainty and accountability.	The Authority disagrees with CCTL's recommendation to make Guideline, now measure, 13, "Incident Response Capability and Preparation", a recommended guideline. Responding to cyberattacks is key to ensuring that priority is given to cybersecurity throughout the industry for the protection and best interest of customers and stakeholders, as required, in accordance with section 3 of the Act.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				requirements for incident capability and submission of security plans are legislated and could therefore be determined by a regulator as conditional to a concession. Compared to the CB Guidelines, these Guidelines are not situate among authoritative legal sources to achieve cybersecurity objectives and may therefore lead to incoherence. But given the general spirit of this language, CCTL implores the Authority to consider all Guidelines as voluntary mechanisms while facilitating the sector's interests, and for providers of critical cyber systems, in broader cybersecurity legislation.		
67	4.6	Development and maintenance of cybersecurity plans	CCTL	Guideline 14 & 15: CCTL firmly believes that acknowledging the existence of a plan via independent certification is appropriate, but requiring its submission for approval is not. A network security plan is a highly sensitive, confidential document containing threat assessments, vulnerability data, and response procedures. Its effectiveness depends on its confidentiality. Mandates on these matters in the absence of a clear legal basis remains questionable. Mandating the submission of network security plans for approval to the Authority whereby competence in cybersecurity is uncertain and	CCTL recommends that TATT eliminates references to the submission of network security plans in Guideline 14.	CCTL is asked to note that operators may submit to the Authority their cybersecurity plan or "suitable independent certification of the existence of their cybersecurity plan". The option to submit the plan is included for cases where an operator may prefer to submit the plan versus submitting a suitable independent certification of its existence.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				beyond regulatory purview creates a central point of risk. This requirement contradicts the core security principles of least privilege and zero trust, which CCTL previously raised. Regarding Guideline 15, while CCTL actively incorporates threat intelligence into our planning, mandating alignment with a single national body's threat assessment is too rigid. Effective security relies on diverse intelligence sources. Cooperation with entities like TT-CSIRT is most effective when it is voluntary, confidential, and occurs within an established trust community that will set its own protocols for exchanges.	CCTL further recommends that Guideline 15 be reconfigured to encourage voluntary cooperation with TT-CSIRT, allowing competent and duly authorised representatives of operators to establish their own agreements and protocols among themselves within a trust community.	The Authority does not intend to approve cybersecurity plans but will review them, to ensure that elements related to network development and the quality of service provided by network operators in relation to the mitigation of cyberattacks are included. Guideline/measure 15 requires operators to update their cybersecurity plans, to ensure they are relevant to the threat assessment of TT-CSIRT or other recognised cybersecurity authority. Guideline, now measure, 19 recommends the sharing of information between TT-CSIRT and the operators, and between operators. Mechanisms and agreements between the parties should be established, to allow for the sharing of cybersecurity information.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
68	4.7	Incident reporting	CCTL	Guidelines 17-20: CCTL acknowledges the Authority's consideration of providing further qualification to incidents.	To ensure a clear and consistently applied standard, CCTL strongly recommends that the Authority work with operators to establish a precise, tiered definition of a "significant incident" based on objective criteria (e.g., number of customers impacted, specific types of data compromised, duration of service disruption), as CCTL initially proposed.	The Authority disagrees with CCTL's recommendation to establish a precise, tiered definition of a "significant incident" based on objective criteria, such as the number of customers impacted, specific types of data compromised and the duration of service disruption. Non-significant cybersecurity incidents may refer to incidents that were detected by security detection and monitoring platforms and proactively extinguished before any network element or service was compromised, while significant cybersecurity incidents refer to full cyberattacks, where services were either adversely affected or impaired; and user information or network elements were compromised. Criteria, such as the number of customers impacted, specific types of data

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						compromised, and the duration of service disruption, will be included in reports related to cyberattacks submitted to the Authority by the operators. These reports are only required by the Authority when a significant cybersecurity incident has occurred.
69	4.8	Supply chain and vendor management	CCTL	Guideline 21: The Guideline remains broad and is void of supplier tiers. Standards within this Guideline should be subject to public consultation and aligned to international standards.	Through another instance of consultation, CCTL proposes that operators be allowed to define "significant vendor arrangements" based on their own comprehensive risk assessments, which would then determine the level of scrutiny applied. This is a more scalable and efficient approach than applying a uniform standard to a wide array of vendors.	Guideline/measure 21, "Supply Chain and Vendor Management", is recommended and broad, which allows operators and broadcasters to develop their own "significant vendor arrangements" based on their risk assessments with their vendors.
70	Appendix II	Appendix II: Template for the Reporting of Compliance with	CCTL	The Authority's decision here contains a direct contradiction to its decision in Item 10 of the Addendum. If, as the Authority states, operators are permitted to define their own thresholds, then it is logically impossible to create a fair or meaningful public score, grading or ranking. An operator that sets a high internal bar for compliance may report	CCTL reiterates its call for clearer language, precise definitions, and the abandonment of publishing compliance reporting.	The Authority is of the view that its language in the Cybersecurity Guidelines/Framework is clear and the definitions are sufficiently precise.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
		Cybersecurity Guidelines		"partially compliant" on a measure, while another with lower standards reports "fully compliant." The resulting public score would be arbitrary and dangerously misleading. This reinforces our position that the ambiguity of the guidelines and the plan to publish compliance scores are fundamentally incompatible and create an unworkable framework.		The Authority disagrees with the suggestion to abandon publishing compliance reporting. 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.
71		Closing Comments	CCTL	CCTL thanks the Authority for the opportunity to submit these comments to the second round of consultations on the Guidelines and asks that continued dialogue be pursued with industry to eliminate ambiguities to the greatest extent possible, while balancing interests that contribute towards effective cybersecurity.		The Authority thanks CCTL and shares its view in this regard.
72		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 thanks TSTT for its feedback on the Cybersecurity Guidelines/Framework.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
73	4.8	Supply Chain and Vendor Management	TSTT	Recommendation 21 states that "Operators of public telecommunications networks and broadcasting facilities should establish and implement appropriate mechanisms to ensure their significant vendors, and the equipment, software and systems supplied, are secure and are monitored to ensure continued security, in accordance with standards that may be established by the Authority." While TSTT supports the intent of Recommendation 21, we are concerned about the reference to future, undefined standards "that may be established by the Authority." The absence of clarity around these prospective standards creates uncertainty and may pose compliance challenges for operators. We strongly recommend that any such standards be internationally recognised and, most importantly, subject to public consultation with relevant stakeholders prior to their adoption. To ensure consistency, transparency, and interoperability in cybersecurity practices, we suggest aligning with established and widely accepted frameworks such as those developed by ISO (International Organisation for Standardisation), GSMA (Global System for Mobile Communications Association), 3GPP (3rd Generation Partnership Project), and ITU (International Telecommunication Union).	TSTT strongly recommends that any standards referenced under Recommendation 21 should be internationally recognised and subject to public consultation with relevant stakeholders prior to adoption.	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, including with the development of this Framework. The Authority ensures that the standards it adopts are aligned with those developed by globally recognised bodies, such as ISO (International Organization for Standardization), GSMA (Global System for Mobile Communications Association) and ITU (International Telecommunication Union).

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
74	4.6	Development and Maintenance of Cybersecurity Plans	TSTT	TSTT maintains that the submission of cybersecurity plans should be strictly limited to elements that fall within the scope of Section 24(1)(a) of the Telecommunications Act, specifically those related to network development and quality of service. These plans should be submitted for informational purposes only and should not require the Authority's approval. TSTT further emphasises that such submissions should be treated as a reasonable regulatory endeavour, not as a concessionary obligation. We thank the Authority for confirming that only aspects within the scope of Section 24(1)(a) may be subject to revision; however, cybersecurity remains a dynamic and highly specialised field, and the has not demonstrated that it possesses the in-house technical capacity to meaningfully validate or approve such plans. Operators must retain the flexibility to update their cybersecurity measures without unnecessary regulatory delay. Additionally, TSTT reiterates that compliance status must be treated as confidential. Even high-level disclosures risk undermining the integrity of an operator's security posture and may expose vulnerabilities to malicious actors. The Authority must avoid any approach that could publicly signal the strength or weakness of concessionaires' cybersecurity frameworks. TSTT therefore urges that the treatment	The Authority should limit the requirement for cybersecurity plan submissions to elements expressly covered under Section 24(1)(a) of the Act, treat such Authority submissions as a reasonable regulatory endeavour rather than a concessionary obligation, and maintain the confidentiality of compliance status in all forms.	The Authority does not intend to approve cybersecurity plans but will review them to ensure that elements that fall within the scope of section 24 (1) (a) of the Act, specifically, those related to network development and quality of service, are adequate. If the elements of a plan that are related section 24 (1) (a) of the Act are found to be inadequate, the Authority will request the operator to revise the plan accordingly. 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 making available the extent of operators' compliance with the

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				of cybersecurity obligations remains proportionate, clearly within legal bounds, and responsive to the operational realities faced by network operators.		guidelines/measures, consumers are provided with information that would enable them to choose a service in relation to the protection of their interests. While the Authority will not provide details of the specific guidelines/measures with which each operator has complied, the Authority will advise members of the public on the extent to which an operator is conformant with the cybersecurity measures, on a summarised basis.
75	4.11	Monitoring and Compliance	TSTT	TSTT acknowledges the Authority's revision to accommodate operator-specific implementation timelines and welcomes the opportunity to propose a timeframe. TSTT maintains its position that compliance status must remain confidential. TSTT respectfully disagrees with the rationale that publishing compliance status serves consumer protection. The Authority's responsibility to promote the interests of customers must be balanced against the need to safeguard operators' network infrastructure. Compliance with	The Authority should treat compliance status as confidential information. It should not be published in any form, including high-level summaries, without the express consent of the operator. Disclosure of such information poses unnecessary security and reputational risks and does not meaningfully contribute to consumer protection.	The Authority disagrees with TSTT that advising members of the public on the extent to which an operator is conformant with the cybersecurity guidelines/ measures on a summarised basis does not meaningfully contribute to consumer protection. The effect of a cyberattack can be harmful to a consumer and providing consumers with a basic summary of the status of an

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				technical or cybersecurity-related guidelines does not equate to service quality or customer experience in any meaningful or measurable way. Publicising an operator's compliance status, even in summary form, risks misleading consumers, undermines commercial fairness, and creates unnecessary security exposure. Consumer protection cannot be reasonably advanced by disclosing information that is not designed for public interpretation, especially where such disclosure could compromise the very networks that support the services customers rely on.		operators' cybersecurity conformance will help protect consumers. The Authority will not be publishing details of an operator's cybersecurity posture, as this will increase security risks. The level of conformance being shared is just a summary and will not create a security risk. A cyberattack is a reputational risk. The response to addressing a reputational risk is not to withhold conformance information but to increase conformance.
76	Appendix II	Appendix II: Template for the Reporting of Compliance with Cybersecurity Guidelines		TSTT notes the Authority's position that operators are required to submit a proposed timeframe for implementation of the cybersecurity guidelines alongside their cybersecurity plan. However, TSTT maintains that what constitutes a "reasonable" timeframe should not be unilaterally determined by the Authority. Rather, it should be the outcome of a mutual agreement between the operator and the Authority, taking into account the operator's specific	The guidelines should be amended to reflect that implementation timelines must be agreed upon between the operator and the Authority, rather than being subject to the Authority's sole determination.	The Authority agrees that implementation timelines should be agreed upon between the operator and the Authority. Section 4.11 of the Cybersecurity Framework/Guidelines has been revised accordingly, to reflect this, as follows:

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				network environment, internal processes, and resourcing requirements.		"Timeframes for complying with a required measure or conforming with a recommended measure, to which operators currently do not adhere, will be determined in collaboration with the Authority."