Addendum to Decisions on Recommendations from the First of Two Rounds of Public Consultation on the Guidelines for Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities

The following summarises the comments and recommendations received from CCTL during the first of two rounds of public consultation on the *Guidelines for Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities*. These decisions made by the Telecommunications Authority of Trinidad and Tobago (the Authority) are now being issued as the Authority was not aware of CCTL's submission until after the issuance of the second round of consultation. The Authority nevertheless expresses its thanks for all comments and recommendations submitted by CCTL.

The content of this Addendum should be read as part of the DoRs issued on 21st May 2025.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
1	Introduction		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. CCTL would like to thank 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 is of the view that the Guidelines make 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.	CCTL believes that the gaps between public safety goals and TATT's mandate for maintaining consumer protection should be acknowledged and would therefore suggest that these Guidelines be refined to appropriately meet duly intended aims in the absence of broader cybersecurity objectives obtaining at law. CCTL suggests that the Guidelines be reconfigured to reflect an up-to-date iteration of good cybersecurity management principles that operators may adopt, noting the current approach of recommendations and requirements creates unfortunate confusion. Furthermore, CCTL	The Authority refers CCTL to section 1.1 of the document which speaks to the relationship between these guidelines and broader national cybersecurity objectives, and section 2 which captures efforts by regulators in other sectors to ensure related cybersecurity concerns under their remit are addressed. Notably, the works of the Central Bank of Trinidad and Tobago in this area and the International Telecommunication Union recommendations for information security, of which cybersecurity is a subset, for

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				CCTL observes that the Guidelines are anchored to TATT's existing powers as regards the Telecommunications Act 2004 as amended and further notes that TATT's linkages to the National Cybersecurity Framework and particularly the 2012 National Cyber Security Strategy are not expressly evident. Without prejudice to the Guidelines' intents and purposes, CCTL believes that the scope and details of the proposed requirements and recommendations may be incongruous to TATT's mandate of consumer protection in some respects but certainly ideational regarding public safety. Clear distinctions must be made between: i. principles that provide a reasonable and acceptable level of security, which also contribute to digital trust: and ii. confidential measures that keep all stakeholders' interests safe upon which the effectiveness of security depends. Additionally, as one of many examples, nuances among network security, information security and cybersecurity should be duly recognised and asserted as such because these terms are not interchangeable. CCTL has generally noted shortcomings regarding	proposes that these Guidelines be accompanied by adequately defined taxonomy to enhance their precision and minimise uncertainty in providing guidance.	telecommunications organisations, both give credence to the approach employed by the Authority in this document. The Authority welcomes and CCTL is encouraged to detail specific recommendations and propose the up-to-date iteration of good cybersecurity management principles, and the taxonomy that it considers adequately defined, which it would like to see reflected in the document. The Guidelines as issued contain clear and citable definitions under section 1.9 for terms used throughout the document. Also, the approach of recommendations and requirements are not new, as similar concepts have been used in previously published technical standards (that is, mandatory and discretionary standards). The notation for recommendations

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				specificity, expected outcomes and timelines, future proofing for emerging threats and trends, appropriate legislative and policy anchors, and clear interpretations of technicalisms. CCTL believes that effective cybersecurity is a shared responsibility, which does not diminish the need to establish very precise roles and responsibilities for competent actors. For this reason, CCTL asserts that the Guidelines should be designed to serve as an up-to-date iteration of good cybersecurity management principles that operators may adopt to ensure the confidentiality, integrity and availability of public telecommunications networks and broadcasting facilities, cognisant of the role that these assets play in the safety and satisfaction of Trinidad and Tobago's wider society and economy. As it stands, the Guidelines do not present a basis for prescriptive rules as their linkages with public safety actors, other legal and regulatory imperatives, and the wider cybersecurity ecosystem remain unclear.		and requirements is succinctly defined in section 1.10.
2	2	The Cybersecurity Framework in Trinidad and Tobago	CCTL	TATT's illustration of the National Cybersecurity Framework in Trinidad and Tobago reflects de jure instruments for promoting cybersecurity actions within this country, but discounts realities that would have an impact on where these proposed Guidelines should be situate. The 2012 National Cyber Security Strategy is a formidable document that promotes reasonable	CCTL suggests that the Guidelines be reconfigured to reflect an up-to-date iteration of good cybersecurity management principles that operators may adopt, which would add value to existing practices that operators employ as a matter of prudence.	The Authority welcomes and CCTL is encouraged to provide the proposed up-to-date iteration of good cybersecurity management principles that it believes should be stated. CCTL should note that the globally

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				endeavour among concerned actors. Notwithstanding, there is a dearth of actions on which the Guidelines base themselves including, inter alia, the provision of a governance framework for all cybersecurity matters; and the creation of a legal and regulatory framework to maintain order, protect the privacy of users, and criminalise attacks in cyberspace. The National Digital Transformation Strategy 2024-2027 acknowledges that the National Cybersecurity Agenda must be expedited as a matter of national priority, but in general financial and human resources are needed to achieve digital transformation goals. CCTL believes that policy coherence and legal reasoning are crucial to developing adequate Guidelines that can be effective. The Computer Misuse Act 2000 is insufficient to address newer generations of malicious conduct in cyberspace, especially towards modern computer and data systems. While General Privacy Principles are in effect in Trinidad and Tobago, the Data Protection Act 2011 is yet to be fully proclaimed and does not proffer contextual guidance on the responsibilities and procedures of legitimate actors in the event of data breaches or compromises by threat actors. Like the Central Bank of Trinidad and Tobago's (CBTT) guidance for the financial sector, CCTL acknowledges the good intentions of TATT in proposing these Guidelines for the telecommunications sector but is		recognised standards bodies referenced in Section 3 of the document are relied upon worldwide for benchmarking by agencies that employ IT infrastructures. The Trinidad and Tobago Bureau of Standards (TTBS) has also adopted TTS/ISO/IEC 27001, 27002 and 27003 as national standards. The referenced standards and guidelines are updated to reflect the ongoing evolution of information and communications technologies (ICTs) and hence inform organisations of new cybersecurity practices. The Authority notes that there are existing obligations under the current legislation and concessions identified in Section 1.5, which operators are already required to fulfil and thus required to adopt and allow the Authority to pursue the purpose of the document.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				concerned about the absence of requisite critical linkages to fully realise the purported aims of said Guidelines and relevant aims such as the protection of the confidentiality, integrity and availability (CIA) of computer systems and networks.		
3	3	Relevant Global Cybersecurity Standards and Guidelines	CCTL	Having cited these global cybersecurity standards and guidelines, CCTL appreciates TATT's consideration in exploring multiple sources of inspiration for national Guidelines. However, CCTL is unable to discern the relevance of all cited sources in the absence of taxonomy in view of governance gaps, and contextual data highlighting security issues affecting public telecommunications networks and broadcasting facilities at a national level. CCTL acknowledges the benefits of some technical standards and frameworks, which could be considered gold or widely accepted standards vis-à-vis their technical merit, scalability, consistency, interoperability and ostensible applicability to security paradigms. ISO/IEC 27001's guidance towards information security management and systems (ISMSs), and ISO/IEC 27002's iteration of control objectives are universally well-regarded benchmarks despite further requirements for risk and security management that are subject to internal decisions.	CCTL believes that further work is required to establish the criteria for securing public telecommunications networks and broadcasting facilities in Trinidad and Tobago to certify the coherence and relevance of the Guidelines. Said work should depend on critical analyses of security issues in this country, review of existing security management practices, and an assessment of the impacts of current and emerging cybersecurity trends, among other things.	The Authority disagrees that the proposed further analysis is required, since these guidelines speak to best practices that should be adopted regardless of the practices currently adopted. The Authority suggests that concessionaires would need to undertake the requisite internal analysis, based on these best practices. The Authority also held a pre-consultation on these proposed guidelines with concessionaires at which time reservations with meeting the requirements of these guidelines were not raised.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				CCTL is wary about the selection of the cited benchmarks where they may be a prima facie lack of comparability with national contexts considering the administrative implications of same at a time where security governance and legislative framework must evolve and be fit-for-purpose to fully address contemporary challenges.		
4	4	Guidelines for Cybersecurity of Public Telecommunications Networks and Broadcasting Facilities	CCTL	These Guidelines could benefit from a greater appreciation and unequivocal delineations of: i. security management information that can be made public, such as certifications of certain standards to foster digital trust; ii. actions that meet the threshold of compliance for the general benefit of the telecommunications and broadcasting sectors; and iii. confidential practices that are innate to an operator's way of doing business where confidentiality underpins the effectiveness of security measures. CCTL is concerned about the legitimacy of required guidelines considering previously established arguments regarding the positioning of this instrument	Regarding Guideline 1, a clear cybersecurity taxonomy should be developed taking into consideration the current implementation of the National Cybersecurity Framework and the organisational capabilities (OC) of operators to be subject to these Guidelines. Guideline 1 should be proposed with a view to respecting the scalability of requirements in function with an operator's OC, and phased timelines.	The Authority acknowledges that Guideline 1 may have financial implications and, as such, has identified it as a recommended, not required, guideline. Operators who do adopt such standards will be recognised for adoption, but operators are not required to do so if it is not financially viable. On the delineations between security management information and actions that meet the threshold of compliance and confidential practices, these will be assessed on an individual basis in collaboration with operators, as this field is an evolving one, with varying and new scenarios

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				and real legislative and governance gaps in the National Cybersecurity Framework which may undermine the intended aims. Furthermore, CCTL believes that unless there is a greater appreciation of the issues at stake as demonstrated by more nuanced language (e.g. cyber vs network vs information security), and a scale or tiered approach to minor incidents versus significant or serious incidents, or material cybersecurity incidents, the applicability and effectiveness of these Guidelines will be questionable. **Guideline 1:** Adoption of international standard ISO 27001 under the controls specified in ITU-T Recommendation X.1051 may have significant financial and administrative implications, especially for smaller operators.		arising regularly. At the very minimum, operators will be expected to convey any actions they have taken to address a particular guideline. In terms of practices that are innate to an operator's way of doing business and where confidentiality underpins the effectiveness of security measures, the guidelines related to secure information sharing are only recommended. The Authority notes that these delineations are not present in the best practice guidelines observed in other regions and welcomes proposed relevant standards or guidelines that satisfy CCTL's recommendation.
5	4.1	Protection of Critical Network Infrastructure	CCTL	Critical infrastructure (CI) or critical network infrastructure (CNI) and plans for the protection of same are defined and identified at a national level at law in many jurisdictions with mature security governance frameworks. Many of these laws have been conditioned by significant cyberattacks over the years. As CI is not restricted to the telecommunications sector, for the purposes of coherence it would be useful to indicate	CCTL recommends that further attention be paid to sector-specific requirements of CNI protection on the one hand, and alignments to any proposed national plans or concepts of CNI protection.	The guidelines adopted in the document are specific to the critical network infrastructure (CNI) and the core facilities of the telecommunications and broadcasting sectors, respectively. Once broader CNI protection plans are developed,

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				overarching requirements for defending CI against attacks at a national level, which may infer a wider Critical Infrastructure Protection Plan.		the Authority agrees to align to them. However, similar to the guidelines developed by the Central Bank of Trinidad and Tobago (CBTT), the Authority has adopted a similar approach for the telecommunications and broadcasting sectors, until such a broader, national CNI protection plan is established.
6	4.5	Incident response capability and preparation	CCTL	Guideline 13: CCTL's incident response capabilities and practices are reflected in this Guideline. CCTL seeks further clarification regarding the compliance notion of a required guideline in this respect. Given the nature of this subject matter, CCTL disagrees with TATT's likening of "network security plans" to "network development plans" for which TATT has indicated it wants to create a new obligation onto operators and extend its approval capacity to security plans. A distinction must be made between acknowledging the existence of a network security plan, which could be done via various assessments and compliance procedures and submitting for approval a detailed network security plan where TATT's competence on the matter of cybersecurity, information security and network security is uncertain and beyond its regulatory purview despite its citation of Section	CCTL is of the view that this Guideline should be reconfigured as a recommendation to operators given prevailing arguments vis-à-vis TATT's authority and flagrant governance gaps in managing cybersecurity issues at a national level.	The Authority disagrees with CCTL that Guideline 13 should be reconfigured as a recommendation. Network security plans are developed to safeguard users' information from cyberattacks. The ability of a service provider to protect its customers' information is reflected in its quality of service. The Authority maintains that this guideline remains a requirement under the Telecommunications Act, Chap. 47:31 (the Act) and the concession terms and conditions, as stated in section 24(1)(a) of the Act.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				24(1)(a). Cybersecurity goes beyond the telecommunications and broadcasting sectors. In the absence of qualified requirements and specific requests on network or information security, CCTL trusts that TATT may have greater justifications for wanting sensitive and confidential information on which they very effectiveness of security management lies.		
7	4.6	Development and maintenance of cybersecurity plans	CCTL	Guideline 14: CCTL acknowledges TATT's authority under Section 24 (1) (a) of the Act, whereby a concessionaire is required to submit to TATT for approval its plans in relation to its network development, quality of service and any other matter TATT may require. CCTL, however departs from TATT's rationale in considering that given that "cybersecurity preparation involves network development affects the quality of service provided by network operators, operators will be required by the Authority to document their plans and procedures relating to the securing of their networks from cyber threats and attacks, either as part of existing network development and quality of service plans, or as a separate and dedicated plan addressing how the network will be developed and maintained, and quality of service assured in relation to cybersecurity." CCTL believes that TATT's requirement undermines key information security principles, namely least	CCTL recommends that TATT opts for self-assessments and attestations concerning network security plans as opposed to requesting that plans are submitted for approval given the risks that could arise when implementing security measures owing to trust deficiencies and a lack of safeguards. While CCTL sees the value in encouraging informal cooperation, we believe that such cooperation must remain voluntary and confidential within the framework of an established trust community that will set its own protocols for exchanges. This view should not be seen to obfuscate CCTL's duties before competent authorities in the case of	The Authority agrees and advises that Guideline 14 permits operators to submit suitable independent certification for network security plans where applicable, instead of submitting or sharing any confidential or proprietary information. On Guideline 15, the guideline is also necessary to ensure that plans that are developed are relevant to a suitable competent authority's threat assessment. For example, if the Cyber Security Incident Response Team (TT-CSIRT), a division of the Ministry of Homeland Security, indicates that ransomware is particularly relevant, operators

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				privilege and zero trust, which is antithetical to the aims of cybersecurity plans. Confidential, proprietary, sensitive and secret data are integral to an organisation's cybersecurity plans, ergo CCTL would imagine that TATT understands the sensibilities of its proposed "requirement" as currently construed. Arguments to further support the rationale for submitting network security plans for approval are welcome. CCTLs also notes that compliance procedures for the CBTT's Cybersecurity Best Practice Guideline consist of self-assessments and attestations, and the submission of plans for remedial actions where material deficiencies are identified. This approach appears to be more suitable given the intricacies of the subject matter. Guideline 15: Regular reviews of security plans are intrinsic to CCTL's management processes, the impetus of which is our commitment to our customers in an open, competitive market. We also understand the role that the TT-CSIRT may play in managing an incident or event that is deemed a significant or serious threat to national security. Such role, however, is distinct from voluntary cooperation with a CSIRT — as with a CSIRT network — to facilitate information exchange and the analysis of detected emerging threats on telecommunications networks.	investigations and/or matters pertinent to national security.	should ensure that plans they develop address ransomware threats. The Authority does not agree that an operator ensuring a cybersecurity plan is relevant to relevant threats should be voluntary.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				CCTL sees that beyond a possible obligation to cooperate on matters germane to the national security interests, informal cooperation mechanisms which are indeed useful to strengthening security, are truly effective through the voluntary commitment of information security professionals within an established trust community like a CSIRT network. Such communities set confidential rules of engagement and protocols under which information is shared. CCTL believes that this Guideline is excessively broad, imprecise and harmful to the aims of security for lack of appreciation of the dynamics of cooperation in the security domain.		
8	4.7	Incident reporting	CCTL	Guideline 17: Whereas CCTL is not opposed to notifying TATT of incidents, the Guideline as currently construed is too broad and is not established in law, which makes its operationalisation impractical and burdensome to operators. CCTL believes that the term "incidents" should be further qualified as it does not consider the distinction between types of incidents such as minor cyber incidents, data breaches affecting customers' personally identifiable data (PII) or material cyber incidents. We are of the opinion that clear distinctions would be essential to determine the appropriate response, notification and mitigation.	Further to introducing a tiered system or criteria for identifying incidents, CCTL believes that TATT should expound on the purposes of incident reporting and more specifically the ways in which same may affect threat mitigation and/or policy making.	Regarding Guidelines 17 and 18, the Authority agrees and provides further qualification under section 4.7 and under Guideline 17. Guideline 18 implies that following a disruption in telecommunications services, the operator provides the Authority with a report which entails a root cause analysis for the disruption, and measures to be implemented to prevent or mitigate any future occurrences. The purpose of the incident

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				Guideline 18: There should be clear consideration of an incident's scale and impact on customers and infrastructure. CCTL reiterates the need for defining the characteristics of an incident that may constitute either a minor cyber incident, a serious data breach affecting customers' PII or a material cyber incident. CCTL is concerned about sharing broad sets of information outside of pre-established protocols as those which obtain within trust communities given that such actions may work against threat mitigation and the overarching goals of a security plan. Notwithstanding, CCTL would acknowledge the importance of cooperation with competent authorities for investigative purposes, or within the rubric of a matter deemed critical to national security. However, as previously stated, such governance framework is underdeveloped in Trinidad and Tobago at this time. Guidelines 19 & 20: Threat warning systems and privileged information sharing are typical features of CSIRTs, making an organisation's affiliation with multiple CSIRT networks a strategic decision to bolster the effect of their internal measures. However, caution must be paid to voluntary affiliation versus a mandatory action, established at law, for which the latter could arise from a statutory interpretation of critical infrastructure in relation to guaranteeing public safety		report will be to inform the Authority of the cyberattack, as well as allow relevant agencies, such as TT-CSIRT, to evaluate whether its threat assessment needs to be updated. Guidelines 19 and 20 are recommended guidelines that the Authority encourages operators to adhere to, but it acknowledges these are not currently required by law and therefore are only recommended. TT-CSIRT has developed a framework for information sharing, but an operator can choose to not partake at this time.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				and/or acting tactically in response to a situation of national interest. These Guidelines do not reflect a profound appreciation of the complex relationships and conditions that provide the premise for effective cybersecurity management at a national level. CCTL is of the view that the Guidelines in general cannot provide a panacea for the previously mentioned governance gaps but would understand their promotion to be a reasonable endeavour among operators within the specific context of enhancing cybersecurity. CCTL registers its concerns with the notion of sharing sensitive and confidential information outside of a framework established by a competent authority and without sufficient legal basis where strong safeguards are absent concerning managing incidents with privacy and CIA implications or limiting liability when an operator complies with a procedural matter of a competent authority such as fulfilling a production order. As currently construed, CCTL believes that implied data and information exchanges among indicated parties could inadvertently lead to further serious compromise in the absence of safeguards.		
9	4.8	Supply chain and vendor management	CCTL	Guideline 21: The Guideline broadly recommends that operators assess and manage cybersecurity risks associated with third-party vendors or service providers. The Guideline is void of supplier tiers to be	CCTL seeks clarifications on the interpretation of significant vendor arrangements and suggests that the Guideline be reconfigured to address	The Authority clarifies that for vendors who supply goods and services relative to the security layers within a network (ITU-T

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				considered and is furthermore short of defining significant vendor arrangements to better qualify the risks to be considered. Given the volume and matricial complexity of third-party relationships with operators, this recommendation will be logistically challenging to achieve resulting in operational burden.	a subset of vendors based on clear criteria linked to extant law such as public procurement.	X.1205), cybersecurity risk assessments should be conducted and the necessary security measures implemented.
10	4.11	Monitoring and Compliance	CCTL	TATT indicates that the status of compliance for these Guidelines should not be considered as confidential information but rather as information that should be known to consumers and may be published by the Authority. CCTL urges TATT to revisit this consideration given the sensitivities involved in effective cybersecurity management. TATT should make a clear distinction of actions that build digital trust, for which consumers should be made aware, and publishing the status of operational security tasks as the latter will indubitably augur risks for operators. CCTL kindly suggests that TATT strike the right balance between compliance health and visibility, such as actions that build digital trust, and confidential practices and information that are innate to effective cybersecurity management. For risk reasons, CCTL is unable to support TATT's proposed compliance publications and seeks further clarification on the purposes of reporting.	CCTL recommends that TATT revisits the purposes of reporting and clarifies its intentions regarding building digital trust versus facilitating effective cybersecurity management given that the proposed aims for compliance, as currently stated, are counterintuitive.	Reference is made to sections 3 (c) (iii) and 3 (c) (iv) of the Act; where the objectives of the Act include providing for the protection of customers of telecommunications services and promoting the interests of customers in regarding the quality and variety of telecommunications services offered. By publishing the extent of operators' conformance with the guidelines, consumers are provided with more information that would enable them to choose a service that will protect their interests. As articulated in the second paragraph in Section 4.11, the Authority does not intend to provide the details of

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
						those specific guidelines with which operators have complied, but generally a summarised score, grading or ranking of the level to which conformance has been achieved, to allow consumers to make informed decisions without exposing operators to unnecessary risks.
11	Appendix I	Appendix I: Template for Reporting of Cybersecurity Incidents	CCTL	As previously mentioned, CCTL could appreciate the value of reporting a serious data breach or compromise, or a material cybersecurity incident given the gravity of their implications for customer protection and the CIA of public telecommunications networks and broadcasting facilities. Documenting certain cyber incidents is indeed crucial to formulating further advice on common measures to be taken at a national level. CCTL is uncertain of TATT's expectations of this report and the report's relevance to operational cybersecurity matters whereby the national cybersecurity management ecosystem is currently underdeveloped. There should be clear delineations of matters that are telecoms-specific and demonstrated ties to other concerned regulatory areas.	CCTL believes that this Template should be restricted to specified instances, in the interest of preserving integrity before customers and other key stakeholders. TATT should avoid creating reporting burdens should minor and insignificant incidents occur with little to no material impact on customers, public networks or broadcasting facilities.	Appendix I – the Authority agrees with CCTL and informs CCTL that section 4.7 and Guideline 17 have been revised accordingly to reflect the reporting of significant incidents only, i.e. any meaningful cybersecurity incident.
12	Appendix II	Appendix II: Template for the Reporting	CCTL	Ambiguity with the compliance notion and other terms remains unsettling.	CCTL suggests that TATT reviews, inter alia, compliance notions, language clarity and precision, and	The Authority has defined the difference between recommended and required,

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
		of Compliance with Cybersecurity Guidelines		The choice of recommended versus required appears arbitrary, as the substantive issues are not broken down according to a rationale beyond the action areas listed in accordance to the 2012 National Cyber Security Strategy and TT-CSIRT objectives. CCTL would like to get a further explanation on the intention of a required Guideline and its implications for compliance if no national cybersecurity directive has been set in this regard. Clarity in Compliance Notion The "Compliance Notation" column mentions the use of (✓) to indicate compliance, but it isn't clear how to use this notation for partial compliance or non-compliance. This column needs clearer instructions. A suggestion would be to have checkboxes or a clearer scale (e.g., "Fully Compliant," "Partially Compliant," "Non-Compliant" with corresponding checkboxes or numeric scores). There is also the question of how "Partially Compliant" or "Non-Compliant" scenarios are reported and addressed. It would be useful to include a space for explanations or action plans to remedy non-compliance. Clarity in Guidelines	compliance timelines. CCTL reiterates the need for reporting purposes to be conceptualised beyond bureaucratic requirements in light of the specific requirements of effective cybersecurity and shared roles and responsibilities within and among actors on this matter.	where required guidelines are subject to existing obligations under the Act or concessions. The Authority believes that placing the check indicator under the appropriate column to indicate full, partial or non-compliance is self-explanatory. As this is a template, an operator can elect to include comments in any of the entry fields or add a comments column to the right of the table for additional commentary. The guidelines that are broad are intentionally broad, as illustrated in other standards and best practice guidelines published, which do not specify particular metrics or tools. Operators are required to demonstrate how a guideline has been met and are permitted to define their own thresholds based on their own networks and risk assessments.

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
				Several guidelines are broad, such as "Operators should monitor network traffic to detect malicious behaviour" (Guideline 4) and "Operators should maintain security information and event management systems" (Guideline 6). Specific examples, metrics, or tools would help operators understand what is expected for compliance. The recommended guidelines are especially vague and could benefit from more detailed examples or best practices. Clarity in Timelines for Compliance Some guidelines do not specify when compliance is expected. For example, there is no deadline mentioned for ensuring that security systems are maintained at their most secure versions (Guideline 2). Guidelines with a "Required" status should include specific timelines for compliance to avoid confusion and ensure timely action.		The Authority acknowledges that operators will require time to implement the guidelines. As indicated under Guideline 14, operators will be given a year to submit to the Authority their cybersecurity plan or evidence of its existence. In addition, operators are encouraged to 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 that are advanced in their security arrangements can achieve conformance in a shorter timeframe than operators with less security measures in place.
13		Closing Comments	CCTL	CCTL looks forward to further engaging in this process.	CCTL implores that TATT revisit the numerous nuances, ambiguities, and gaps in the Guidelines as currently construed and further argues that proposed guidelines serve as an up-to-date iteration of good cybersecurity	The Authority welcomes CCTL providing the up-to-date iteration of good cybersecurity management principes that operators may adopt. The Authority is not clear on the

Item	Section	Section Title	Stakeholder	Comments	Recommendations	TATT's Decision
					management principles that operators may adopt. CCTL would like to highlight the differences between CBTT's and these Guidelines vis-à-vis compliance procedures and suggests that TATT considers innovative ways in promulgating principles considering governance gaps and absent linkages with the National Cybersecurity Framework.	differences CCTL would like to highlight between CBTT's guidelines and the Authority's, and welcomes clarification from CCTL, particularly as the Authority referenced CBTT's guidelines in formulating its own.