High Level Comparison Table: TICA 2004 and TICS Bill

	TICA 2004	TICS Bill 2013
Interception capability duties (Part 2)		
Obligations on network operators to have interception capability	All network operators are required to ensure their public telecommunications networks and their telecommunications services are interception capable (**NB** the full obligation applies irrespective of the size or type of network operator, or operational need for capability).	Some network operators are required to ensure their public telecommunications networks and their telecommunications services are interception capable. However, **reduced obligations** can apply to: • network operators with fewer than 4,000 customers (an average over a six month period) • network operators offering wholesale network services • network operators offering infrastructure-level services. Ability to reinstate obligations (to the full capability obligation) for network operators if required for operational reasons, following a clear process. ➢ **More targeted, proportionate obligations on network operators**
Exemptions from interception capability obligations	The **Minister** responsible for the administration of the Act may exempt any network operator from interception capability requirements if **special circumstances** exist (for example, a pilot trial of a new network or telecommunications service) that justify granting an exemption.	A **designated officer** (or the **Minister**) may exempt a network operator (or a class of network operators) from aspects of specified interception capability duties. ➢ **More flexible, and faster, exemption process**
Duty to assist surveillance agencies	All network operators and all services providers are required to take all reasonable steps necessary to assist surveillance agencies in the execution of an interception warrant.	All network operators and all service providers are required to take all reasonable steps necessary to assist surveillance agencies in the execution of an interception warrant – for clarity, examples of what assistance may entail are now explicitly set out. ➢ **Greater clarity about the obligation**
Ability to require		The Minister may require service providers to have the same

service providers have the same interception capability obligations as network operators		capability obligations (one of the tiered obligations) as network operators if there is an operational need, and following a clear decision making process in which service providers have the opportunity to submit. ➢ **Greater flexibility to respond to future operational needs and new technology uses**
New: Formal network security obligations (Part 3)		
Good faith obligation		General obligation for network operators to engage with the GCSB in good faith in relation to proposed decisions, courses of action, or changes that may raise network security risks if they are implemented.
Notification obligation		Requirement to notify the GCSB of certain proposals, decisions and changes at the planning stage.
Process for preventing or sufficiently mitigating network security risks		Process for network security risk identification, response and assessment: • the response to network security risk to be designed and proposed by the network operator, • assessment by the GCSB (but no ability for GCSB to direct).
Ministerial direction power		The Minister responsible for the GCSB may require a network operator to, for example, take steps or cease taking steps, to prevent, or sufficiently mitigate or remove, a significant network security risk (with procedural checks and balances). Before referring the matter to the Minister, the Director of the GCSB must seek an independent review of his or her security assessment by the Commissioner of Security Warrants.

High Level Comparison Table: TICA 2004 and TICS Bill

Joint compliance and enforcement framework (Part 4)		
Compliance measures		New compliance measures: • Network operators to register, and provide basic information. • Information gathering powers to support compliance and enforcement. • Ability to request certification of compliance, and compliance testing (for interception capability only). • Compliance testing (for interception capability only). • Ability to request a security clearance for an employee in certain network operators. ➢ **Increased ability to monitor and enforce compliance**
High Court may issue a compliance order	The High Court may, for the purpose of preventing any further non-compliance with interception duties, make a compliance order requiring a person to do any specified thing; or to cease any specified activity.	New two tier enforcement process. 1. Breach notice (issued by a surveillance agency) for **minor non-compliance** requiring the breach to be remedied within a specified time. 2. High court action for **serious non-compliance** – a compliance order and pecuniary penalty can be issued simultaneously. ➢ **Fit-for purpose, and graduated, enforcement process**
Pecuniary penalties for not complying with the compliance order	Provides for the High Court to order pecuniary penalties be paid for contravention of duties of compliance order.	Provides for the High Court to order pecuniary penalties be paid for contravention of duties of compliance order. ➢ **Level of penalties unchanged**
Provisions relating to classified security information		New provisions relating to protecting classified security information in court proceedings, including allowing information to be presented in the absence of named parties (such as journalists or members of the public), the ability for the court to

		appoint a special advocate to prepare and commence proceedings on behalf of the non-Crown party, and for the court to approve a summary of classified security information. ➢ **Safeguards for non-Crown parties in Court proceedings involving classified security information**