Cyber Security Centre for the Isle of Man

Department of Home Affairs

Rheynn Cooishyn Sthie

PROPOSED NATIONAL INFRASTRUCTURE SECURITY BILL (NISB)

Guide

NISB aims to improve the resilience of the Islands critical national infrastructure, enhancing the protection of our essential services against a cyber attack.

Contents

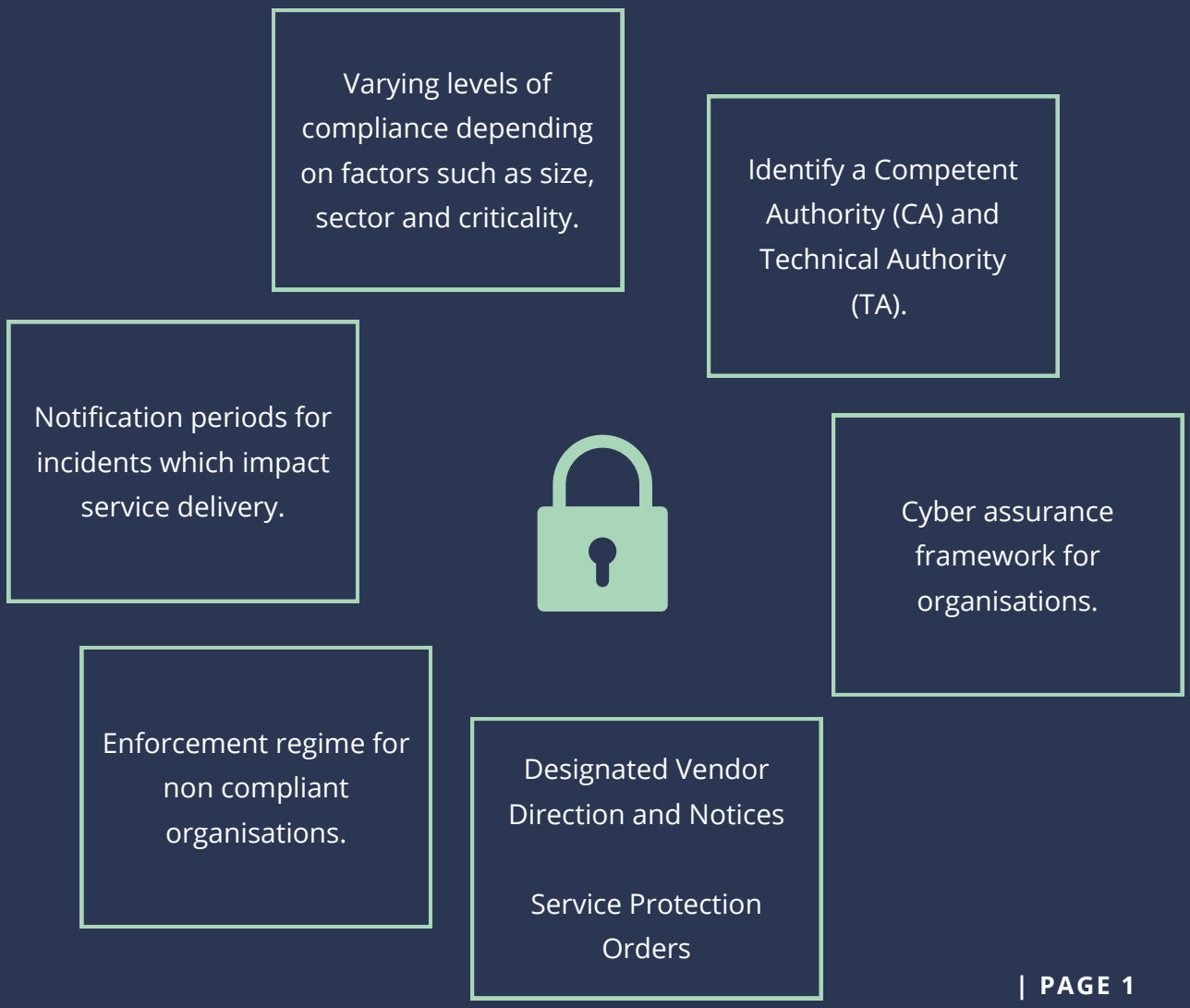
Introduction

Isle of Man residents should have confidence in the security and resilience of national infrastructure sectors to deliver essential goods and services. Essential services provided by both public and private sectors – such as our electricity grid, water supply and telecommunications systems should be able to withstand and recover from hazards that might disrupt their functions.

Unfortunately, hostile entities and criminals have recognised that this dependency creates an opportunity for what have become known as 'cyber-attacks'.

The Department of Home Affairs wishes to introduce a National Infrastructure Security Bill to raise levels of cyber security and resilience for core services on the Isle of Man, which rely heavily on digital services.

The diagram below illustrates some of the core elements of the proposed legislation.



1

WHAT IS THE NATIONAL INFRASTRUCTURE FOR THE ISLE OF MAN?

What systems and assets, including physical, digital, and organisational, are essential to the functioning of the Isle of Man and its economy.

What is the National Infrastructure for the Isle of Man?

One of the policy principles for the proposed National Infrastructure Security Bill (NIS-B) was that the sectors that form part of the Island's National Infrastructure should be identified and included in the scope of the legislation.

For the purposes of this legislation the National Infrastructure means the systems and assets, including physical, digital and organisational, that are essential to the functioning of the Isle of Man and its economy.

The National Infrastructure for the Isle of Man comprises of many elements, commonly known as sectors and within those sectors will be businesses and organisations working to deliver the services upon which we rely.

Within this wide collection of businesses and organisations, known as entities, some will be more critical to our daily lives and the Isle of Man economy than others. Equally some will be larger than others.

Critical National Infrastructure

In introducing any proposed legislation we need to be able to take into account the differences in levels of criticality within the National Infrastructure and the size of the entities who are delivering the services we rely on and apply any requirements in a proportionate manner.

From the research we have conducted we are proposing that the EU Network and Information Security Directive – 2 (EU NIS-2), the UK Network and Information Systems Regulations 2018 and the UK Telecommunications (Security) Act 2021 provide a basis on which we can address these differences.

Taking a similar approach to the EU NIS-2 and recognising some may already be conforming to this in other jurisdictions it is proposed that the Isle of Man's Critical National Infrastructure will be divided into two groups, sectors of High Criticality and Other Critical Sectors. The two groups are shown in the tables on page 6.

Proportionality

Another policy principle for the proposed National Infrastructure Security Bill was that the measures introduced should be proportionate to the needs of the Isle of Man whilst also taking into account the type of service and size of the supplier. In order to ensure the necessary proportionality we are proposing that:

Whilst all entities operating in the Sectors of High Criticality and other Critical Sectors will be required to register with the Competent Authority(ies), there will be:

- Two levels of compliance depending on the size of the entity and the criticality of the service provided
  - These entities would be classed as either 'Essential' or 'Important' and this classification would determine the assurance regime they would be subject to

It is also proposed that the following criteria is used to define the size of an entity:

- Small 5-24 employees
- Medium 25-74 employees
- Large – 75 employees and above

This is explained in more detail in section 3 of this guide – Essential and Important entities.

2

SECTORS OF HIGH CRITICALITY AND OTHER CRITICAL SECTORS

From the results of the consultation held in March of 2024, it is apparent there is a need to classify elements of the National Infrastructure based on their level of criticality, similar to measures undertaken in the UK and EU.

Sectors in Scope

All sectors listed below are critical however, some areas are more critical than others. The proposed approach is to use the EU NIS2 categorisation, in which sectors are divided into two groups: "Sectors of High Criticality" and "Other Critical Sectors".

Further consultation will be undertaken with the sectors who could be subject to the proposed legislation.

1. Sectors of High Criticality

2. Other Critical Sectors

*It is proposed that the legislation will cater for changes to the sectors by allowing for adjustments

3

ESSENTIAL AND IMPORTANT ENTITIES

The designation of 'Essential' and 'Important' will determine the assurance framework an entity will follow. Entities may be designated as 'Essential' or 'Important' depending on factors such as size, sector, and criticality.

Essential and Important Entities

Whilst all entities operating in those sectors deemed to part of the Critical National Infrastructure (as shown in the following tables) will be required to register - only those entities assessed as 'Essential' or 'Important' will be required to adhere to the assurance framework.

The designation of an entity as either 'Essential' or 'Important' informs which level of assurance framework they will be required to follow.

If an entity is categorised as 'Essential' it is because an issue with service delivery could adversely impact public safety, security, health or economic stability. However, an organisations size will also be used to assess whether it is subject to 'Essential' or 'Important' levels of Assurance.

Some sectors are deemed so critical that a designation of 'Essential' is applied for organisations of all sizes. While other sectors feature entities with multiple designations depending on an organisations size.

While EU NIS-2 has set out criteria for classifying entities as either small, medium, or large it was apparent from our research and feedback from the consultation that these would not be appropriate for the Isle of Man. We have therefore proposed new criteria more proportionate for the Isle of Man.

Tables 1 and 2 overleaf illustrate the proposed designations for each sector.

There will be a general duty to adopt cyber security and resilience measures applicable to all registered entities within the legislation.

Annex 1: Sectors of High Criticality

Sector	Description	Large Entities (75 Employees+)	Medium Entities (25-74 Employees)	Small Entities (5-24 Employees)
Telecommunications	Providers of Public electronic communication networks	Essential	Essential	Important
Energy	Electricity: district heating & cooling, Gas: hydrogen: Oil. Incl. providers of recharging points	Essential	Important	Registered Entities
Transport	Air (commercial carriers, airports, ATC; Rail (ecl. Heritage railways); Water: Transport companies; ports; Vessel traffic services; road	Essential	Important	Registered Entities
Banking	Class 1 licence holders under the Regulated Activities Order 2021	Essential	Important	Registered Entities
Health	Healthcare providers; reference laboratories; R&D medical products; manufacturing of basic pharma; manufacture of medical devices critical to PH emergency	Essential	Important	Registered Entities
Drinking Water		Essential	Important	Registered Entities
Waste Water	Only if it is an essential part of general activity	Essential	Important	Registered Entities
Digital Infrastructure	Qualified trust service providers	Essential	Essential	Essential
	DNS providers (excl. Root name servers)	Essential	Essential	Essential

Annex 1: Sectors of High Criticality (continued)

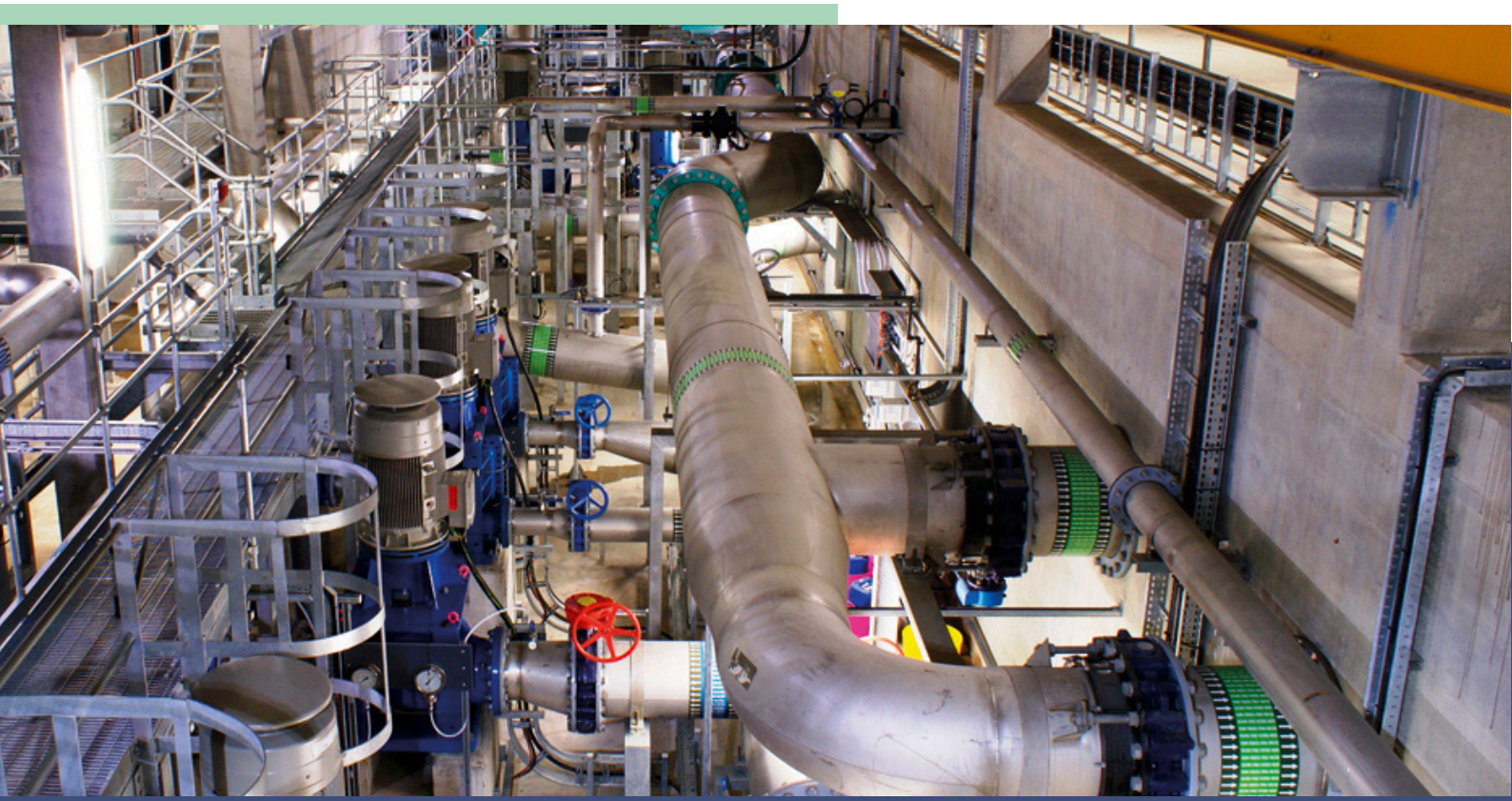
Sector	Description	Large Entities (75 Employees+)	Medium Entities (25-74 Employees)	Small Entities (5-24 Employees)
	TLD name registries	Essential	Essential	Essential
	Non-qualified trust service providers	Essential	Important	Important
	Internet Exchange Point providers	Essential	Important	Registered Entities
	Cloud computing service providers	Essential	Important	Registered Entities
	Data centre service providers	Essential	Essential	Important
	Content Delivery Network (CND) providers	Essential	Important	Registered Entities
ICT service management (B2B)	Managed Service Providers, Managed Security Service providers	Essential	Important	Registered Entities
Public Administration	Central Government (excl. Judiciary, Tynwald,, Defence, national security, public security.)	Essential	Essential	Essential
Space	Operators of ground-based infrastructure	Essential	Important	Registered Entities

Annex 2: Other Critical Sectors

Sector	Description	Large Entities (75+ Employees+)	Medium Entities (25-49 Employees)	Small Entities (5-24 Employees)
Postal and Courier services		Important	Important	Registered Entities
Waste Management	Only if principal economic activity	Important	Important	Registered Entities
Chemicals	Manufacture, production, distribution	Important	Important	Registered Entities
Food	Wholesale production and industrial production and processing	Important	Important	Registered Entities
Manufacturing	(in vitro diagnostic) medial devices, computer, electronic, optical products; electrical equipment, machinery, motor vehicles, trailers, semi-trailers; other transport NACE C26-30)	Important	Important	Registered Entities
Digital Providers	Online marketplaces, search engines, social networking platforms	Important	Important	Registered Entities
Research	Research organisations (excl. educational institutions)	Important	Important	Registered Entities
Entities providing Domain Name registration services	All sizes but with conditions			

4

PROPOSED ASSURANCE FRAMEWORK



A designation of "Important" or "Essential" will determine the level of assurance an entity is expected to comply with.

Proposed Assurance Framework

Depending on an entities designation they will be required to work to a framework to assure the Competent Authority (see section 5) that it is compliant and secure.

The below diagram provisionally illustrates the difference in assurance frameworks that 'essential' and 'important' entities will have to follow.

Essential Entities	Important Entities
Annual Cyber-security & Resilience Risk Assessment and certification	Triennial risk assessment certifcation or post event on demand
Business Continuity Plans	Business Continuity Plans
BCP Annual Testing	BCP Testing
Continuous Improvement Regime	
Identify core service delivery roles and minimum staffing levels	Identify minimum staffing levels
Independent certified compliance every 3rd year	Independent certified compliance post-event as required
Registration of particulars	Registration of particulars
Circumstance change notification (immediate)	Annual verification of particulars
On-site and off-site supervision (incl audits)	Post-event supervision (incl audits)
Information requests	Information requests
Event notification Regime	Event notification Regime

*For registered entities there will be a general duty to adopt cyber security and resilience measures.

5

COMPETENT AND TECHNICAL AUTHORITY

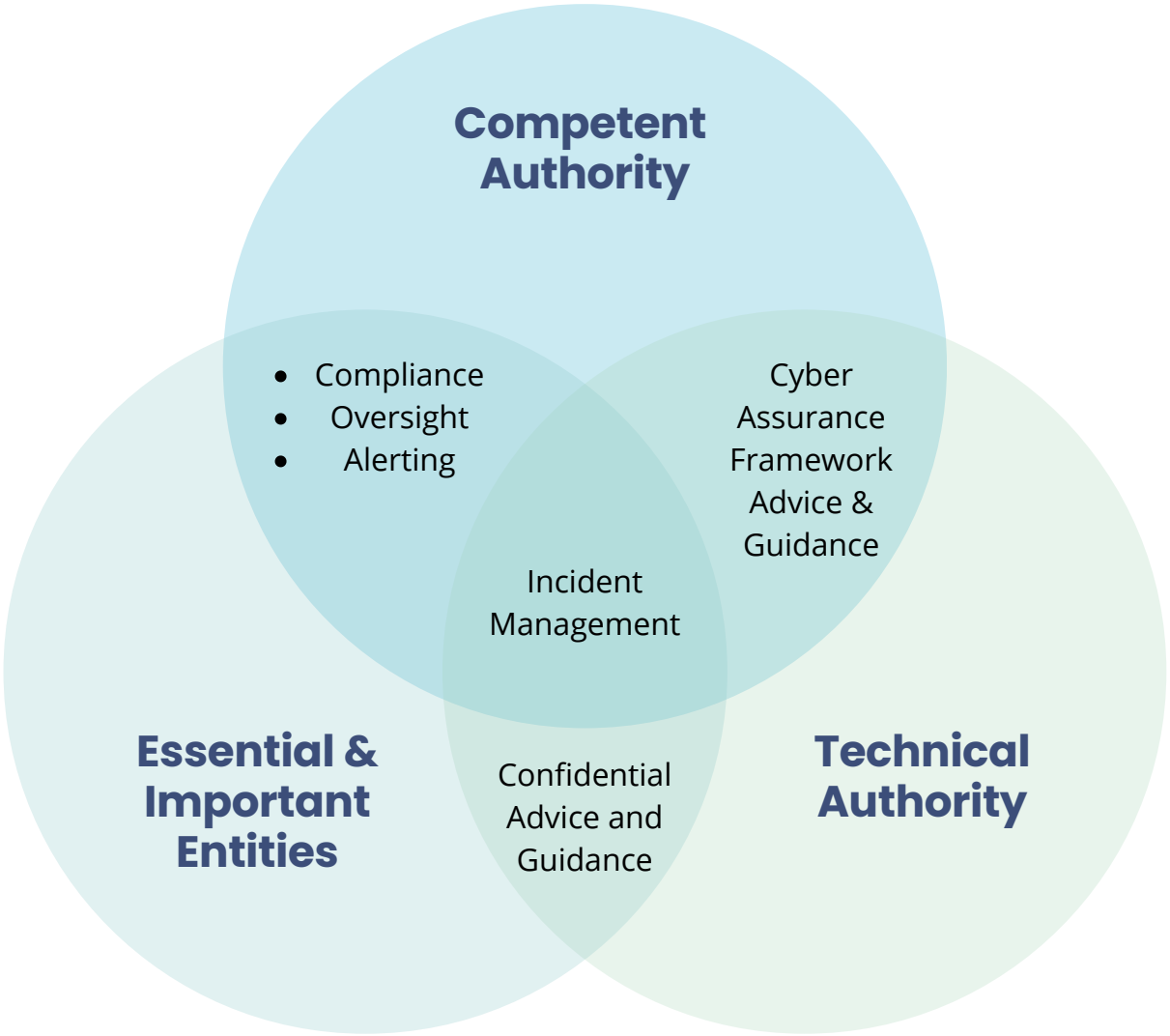
NISB will require the designation or establishment of a Competent Authority, whose purpose will be to ensure compliance with the assurance framework. This Competent Authority will be supported by a Technical Authority.

Competent and Technical Authority

The ability to provide oversight, through the creation of a Competent Authority was supported in the consultation conducted in March 2024. However, there were different views on where the Competent Authority should sit and how this should be operated. The Competent Authority will be advised on matters through a Technical Authority. While it was agreed the Competent Authority should be responsible for the operations of the Technical Authority, the exact structure is yet to be determined.

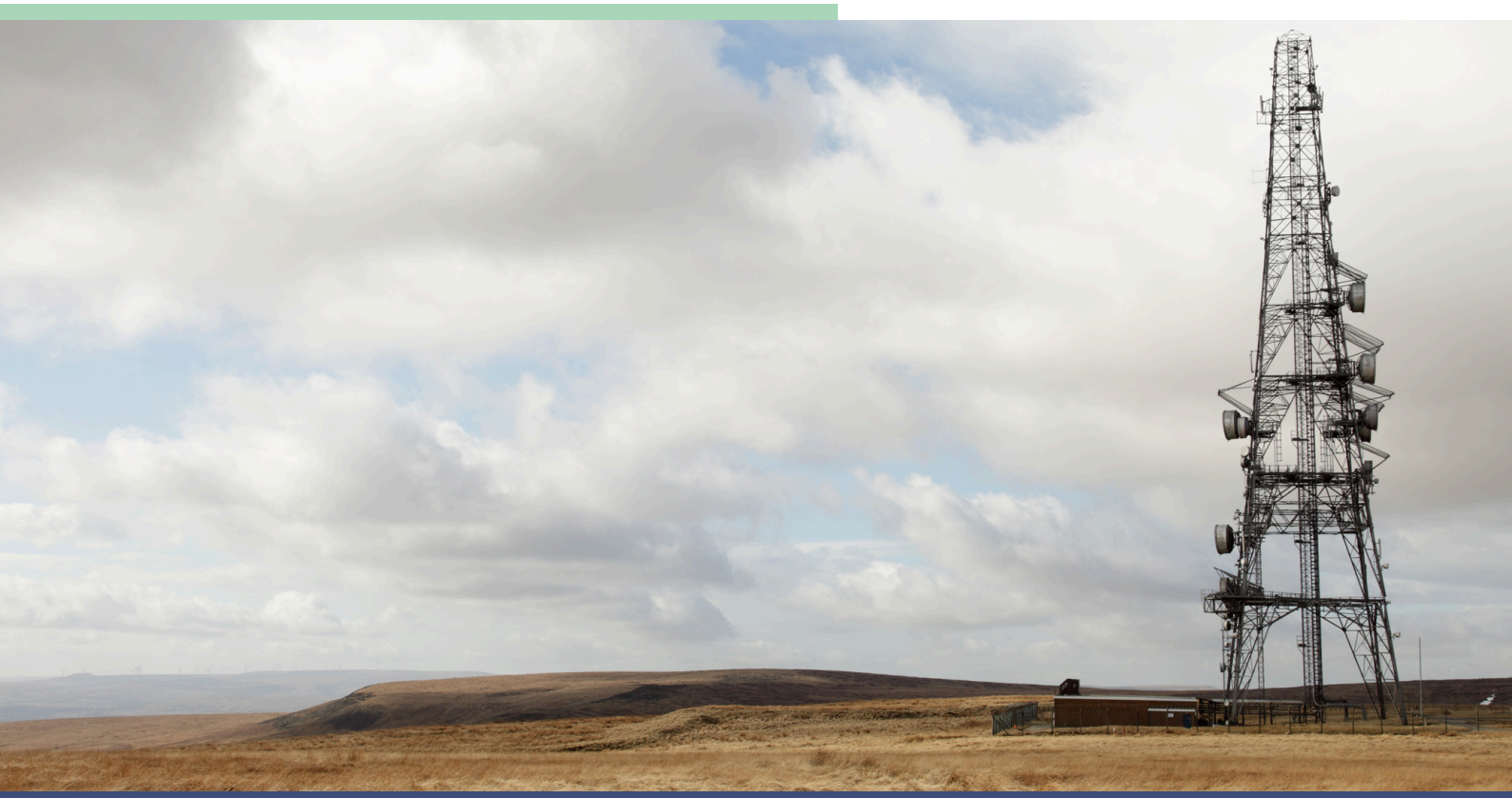
The Department will conduct some further research using examples from other jurisdictions before proposing a model for the Isle of Man.

The diagram below illustrates the relationship between the Competent Authority, Technical Authority and those entities which fall under the scope of the legislation.



6

DESIGNATED VENDOR DIRECTION AND NOTICES AND SERVICE PROTECTION ORDERS



The Government and Competent Authority will have the ability to control or restrict the use of certain equipment for use in the National Infrastructure and to takes steps to protect the services.

Designated Vendors

DESIGNATION OF HIGH-RISK VENDORS

Under the proposed legislation the Government, with the consent of Tynwald, will have the authority to designate a vendor as a high-risk vendor if the vendor is deemed to pose a significant risk to national security and critical infrastructure. Before making such a designation, the Government is required to consult with the competent authority to ensure a thorough evaluation of the potential risks involved.

Should a vendor or entity be deemed high-risk, a direction or notice can be issued.

DESIGNATED VENDOR DIRECTIONS AND NOTICES

The Government has the authority to issue a designated vendor **direction** to essential and important entities. Additionally, the competent authority may issue a designated vendor **notice** to a high-risk vendor, mandating specific actions to mitigate the risks their products or services pose to national security and critical infrastructure.

IMPLEMENTATION

The Competent Authority will be instructed to oversee the implementation of the relevant Directional **Notice** , ensuring the affected entity/entities are compliant.

Service Protection Orders

The Government , with consent of Tynwald, will have the authority to issue a Service Protection Order where it appears that the critical service being delivered by an Essential Entity might be at risk of disruption.

The order, which is only applicable for a short period of time, can require an entity, organisation or other persons to ensure that the critical service named in the order is not adversely disrupted or impacted.

A service protection order may only be issued where there is a risk of disruption to a service delivered in the Sectors of High Criticality by an Essential Entity. It will be supported by a thorough risk assessment and will be timebound,

The Government has the authority to issue a Service Protection Order when there is a real risk of disruption to service of high criticality and the economy, society or national security. The order may instruct those named within the order to take steps to ensure an acceptable level of service is maintained during the period of risk.

Additionally, the order might apply to any other persons not named where any activity undertaken might adversely impact the service being protected.

The Competent Authority will be required to oversee any Service Protection Orders.

7

INCIDENT NOTIFICATION

Entities which fall under the scope of the legislation will be required to report **some** incidents within a certain timeframe.

Incident Notification

NISB will impose notification obligations in phases, for incidents which may have a 'significant impact' on service delivery. These notifications must be made to the relevant competent or technical authority, depending on final legislation.

ASAP

EARLY NOTIFICATION

When an entity **suspects** a potential threat that **may** impact services or National Infrastructure, they must promptly notify the competent authority with relevant details.

Within 24 hours

REPORT

When a risk or event **affects** or is **going to affect** service delivery or National Infrastructure, they must promptly notify the competent authority with relevant details, including any additional information within 24 hours.

Within 72 hours

INTERIM REPORT

to be provided within 72 hours of an event or as required by the competent authority together with as much relevant information as might be required or requested by the competent authority.

As Requested or When Available

UPDATE REPORT

where new or relevant information becomes available or is reasonably requested by the competent authority.

Within 1 Month

FINAL REPORT

to be submitted within 1 month of event closure

As required, the Competent Authority **may** inform other entities whose service delivery may be impacted whilst maintaining levels of confidentiality.

Glossary

Competent Authority (CA)	the body or bodies designated to have regulatory powers
Cyber Assurance Framework (CAF)	an approach to assessing the extent to which cyber risks to essential functions are being managed by the organisation responsible
Computer Security Incident Response Team (CSIRT)	The Computer Security Incident Response Team (CSIRT) is a team charged handling cyber-security incidents.
Critical National Infrastructure (CNI)	the critical systems and assets, including physical, digital, and organisational, that are essential to the functioning of the Isle of Man and its economy
Designated Vendor Direction	a direction issued by the Minister
Designated Vendor Notice	a notice issued by the competent authority
Essential Entities	entities operating in sectors identified as essential for the maintenance of critical societal and economic functions, including energy, finance, health, transport, water and digital infrastructure;
High Risk Vendor	means a vendor who poses a significant risk to national security and critical infrastructure;
Important Entities	entities operating in sectors identified that are essential for the provision of public services or have a significant impact on economic activity;
National Infrastructure	means the systems and assets, including physical, digital, and organisational, that are essential to the functioning of the Isle of Man and its economy
Network and Information Security Directive (EU NIS2)	The NIS2 Directive is the EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU.

Glossary

Network and Information Systems Regulations 2018 (UK)	Provides legal measures to boost the level of security (both cyber & physical resilience) of network and information systems for the provision of essential and digital services.
Resilience	the ability of the national infrastructure to resist, absorb, recover from, and adapt to adverse events and disturbances.
Service Protection Orders	an order issued by a Minister requiring certain steps to be undertaken where it is anticipated that a change of circumstances in connection with an entity or entities might adversely impact service delivery
Technical Authority (TA)	expert-based advice and guidance in all aspects of cyber-security.
Telecommunications (Security) Act 2021	Requires telecoms providers, overseen by Ofcom, to design and manage their networks to protect against existing and future threats to the UK's network security

Disclaimer

The material in this document is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances. OCSIA accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Open Government Licence

CSC Cyber Security Centre for the Isle of Man

Department of Home Affairs
Rheynn Cooishyn Sthie

Office of Cyber-Security & Information Assurance
2nd Floor
Former Lower Douglas Police Station
Fort Street
Douglas
Isle of Man
IM1 2SR

T: +44 1624 685557

Isle of Man Government
Reiltys Ellan Vannin