Consultation on Policy Principles: National Infrastructure Security Bill (NISB)

Closing Date: 25th March 2024

Douglas City Council Response

OVERVIEW

Isle of Man residents should have confidence in the security and resilience of national infrastructure sectors to deliver essential goods and services. Essential services – such as our electricity grid, water supply and telecommunication 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', examples of recent attacks are highlighted in appendix 1.

In response to evolving cyber-threats, Governments in other jurisdictions have introduced legislation aimed at strengthening security for the core services they consider to form part of their National Infrastructure. As such, the Department of Home Affairs is looking to introduce the 'National Infrastructure Security Bill' (NISB) to increase our Island's cyber resilience

The Department of Home Affairs wishes to introduce a National Infrastructure Security Bill to raise levels of security and resilience for core services on the Isle of Man which rely heavily on digital services. The Department is seeking views from interested parties on the key policy principles that would be used to draft the National Infrastructure Security Bill.

PRINCIPLE 1

Protection of the Island's National Infrastructure should be supported by legislation.

Examples of Cyber-attacks on National Infrastructure globally have shown that protection from this type of threat has become necessary. Other countries have introduced legislation setting minimum requirements of security and resilience for the sectors that comprise their National Infrastructure.

So what does this mean? We want to ensure that the Isle of Man's National Infrastructure takes the appropriate steps to protect itself from cyber-attack. We want to support the Isle of Man's position as a well regulated jurisdiction. We want to support the Government's strategy of growing the digital economy. We want to prevent interruption to the services provided by the Island's National Infrastructure. We want to have legislation that meets international standards. We want the legislation to be proportionate to the needs of the Isle of Man.

PRINCIPLE 2

Those sectors that form the Island's National Infrastructure should be identified and included in the scope of legislation.

Isle of Man legislation should take account of the different levels of reliance the Island places upon parts of the national infrastructure, with some elements being critical to the maintenance of society and the economy as well as those that are essential or part of an essential supply chain upon which an identified service is heavily reliant.

The NIS 2 Regulation Directive issued by the European Union in January 2023 introduced the concept of Essential Entities and Important Entities that form part of the National Infrastructure. This approach took account of recent threats to service delivery that have been successful by compromising less important parts of the supply chain. The Critical Entities Regulation Directive (CER) introduced a higher level of supervision, identifying those entities that deliver services deemed critical to the delivery of social, economic and government services such as telecommunications operators, electricity generation and distribution, water and gas to name a few.

The UK Government has recently consulted on a revision to their existing Network & Information Systems Regulations with a view to adopting a similar approach. The Government of Jersey have also consulted on the introduction of cyber defence legislation.

QUESTIONS

Question 1

We would like your views on what constitutes National Infrastructure on the Isle of Man.

Listed below are sectors which could be included in the scope of the legislation. Please identify those ones which you feel are part of the Isle of Man's National Infrastructure and add any you may feel have been omitted.

- Energy – including Electricity, Oil and Gas *** Yes**
- Transport – including Air, Sea and Road *** Yes**
- Financial Services – including banking and market infrastructure *** Yes**
- Health – For example, Hospitals, Research and Public Health Laboratories, Primary Care, Mental Health Services, and Social Care *** Yes**
- Blue Light Services – For example, Police, Fire & Rescue, and Ambulance *** Yes**
- Water – drinking and waste *** Yes**
- Digital infrastructure – including Internet Exchanges, DNS[1] providers, Cloud computing, Data Centre services, content delivery networks, trust service providers, electronic communication network providers and publicly available electronic communication services *** Yes**
- Information Communication Technology (ICT) service management (business to business) *** Yes**
- Government – public administration, entities of central government *** Yes**
- Space – operators of ground based infrastructure that support the provision of space-based services – excluding public electronic communications networks *** Yes**
- Postal and courier services *** Yes**

- Waste management *** Yes (Energy from Waste Plant but not recycling)**
- Chemical manufacturing, production, and distribution *** Yes**
- Food production, processing and distribution *** Yes**
- Manufacturing *** Yes**
- Digital providers *** Yes, may need to sub categorise into critical, essential and non-essential**
- Research *** Yes**
- Other (Please specify below)

  National and Civil Defence Services including Coast Guard.

  Space operators – would need additional information on services provided to comment – Yes, if include public services i.e. isp or gps services.

  *** N.B only if quantified and relevant to the National Infrastructure.**

PRINCIPLE 3

The legislation should be equivalent to measures introduced in other jurisdictions whilst remaining flexible to meet the fast paced changes and threats to the national infrastructure.

As already mentioned there is a recognised threat resulting from the global connectivity and reliance on digital services. As a result in many jurisdictions, including the USA, UK, and EU legislation has been introduced to set a minimum level of cyber resilience for critical and national infrastructure services.

The Isle of Man is not immune from different forms of compromise or attack and could find itself impacted by direct or collateral damage. For this reason the Island should look to introduce legislation commensurate to measures introduced in other jurisdictions. The NIS-2 and CER EU Directives provide examples of the legislative measures that apply in Europe. The UK has also based its legislation on the European approach. Consideration should also be given to including parts of the UK Telecommunications Security Act 2021 that are not included in NIS-2 and the CER. The advantage of taking this approach would be that this would allow the Island to demonstrate that it was following international standards and reinforcing its position as a reputable and responsible jurisdiction.

PRINCIPLE 4

Any legislation introduced should be proportionate to the needs of the Isle of Man.

Having defined the sectors that would be in scope, the Isle of Man should introduce legislation that will ensure that the Island's National Infrastructure takes appropriate and proportionate measures to manage the risks posed from cyber-attack and to minimise the impact of incidents to Island businesses and residents.

QUESTIONS

Question 2

Do you agree that the Isle of Man when drafting its own legislation should take into consideration similar legislation introduced in the UK, EU or elsewhere?

Yes.

Question 2 (a)

(If yes)

If you are aware of legislation in another jurisdiction which contains similar policy principles and consider that this might be a good model to review in the preparation of instructions for the legislation, please confirm which jurisdiction and why?

United Kingdom.

Question 2 (b)

Any other comments?

Agree it should be proportionate measures (scalability issue) to manage the risks posed from cyber-attack and to minimise the impact of incidents to Island businesses and residents.

PRINCIPLE 5

A minimum level of resilience and security should be specified for each of the designated sectors of the Island's National Infrastructure.

This could include the introduction of minimum levels of compliance via a Cyber Assurance Framework (CAF) and certification measures to evidence compliance. Any CAF would need to be flexible to meet sector specific needs and risks.

The cyber environment and capabilities of both hostile and criminal actors change rapidly and so a compliance regime would need to be able to reflect the rapid change of risk profile by including enforcement notices, powers to inspect, fine, suspend or deregister.

PRINCIPLE 6

The ability to provide oversight and management of the sectors of the National Infrastructure should be established in order to ensure minimum levels of resilience and security are achieved.

The legislation should include the power to establish one or more Competent Authorities responsible for ensuring compliance with any requirements imposed on the different elements of the Island's National Infrastructure.

The Competent Authority could be established by extending the powers of an existing regulator or empowering an existing Office of Government to provide technical oversight and adequate level of assurance. Approaches taken in the other Crown Dependencies, the UK and the Republic of Ireland should be considered in determining the best approach for the Isle of Man.

QUESTIONS

Question 3

CAFs exist to protect organisations by providing a standardised system of guidelines and best practice. If you are aware of CAFs that might provide a good model to review in the preparation of instructions for the legislation, please confirm which frameworks and why.

NCSC CAF guidance - NCSC.GOV.UK

The Cyber Assurance Framework would definitely need to have the flexibility to balance the risks to national infrastructure security and the costs of meeting the minimum requirements and be based on outcome standards.

Question 4

If a competent authority was to be established, where do you think would be the most appropriate place for this authority to sit and why.

- Government Department (Select one)
- New Statutory Board
- Arm's length organisation **Yes**
- Existing regulator where appropriate
- Other (please specify)

Question 5

Who should provide oversight/monitoring for a competent authority.

- Government department (please specify) **Yes, Cabinet Office**
- Board (public sector)
- Board (public and private sector)
- Board (private sector)

Question 6

Please provide any comments you have in relation to this proposal:

The competent authority will require a depth of experience.

Oversight and monitoring public and private sector board with aim of combining depth of experience with authority of Government policy.

PRINCIPLE 7

Support for the sectors of the National Infrastructure should be provided by the introduction of a threat and incident management capability.

It would be inappropriate to expect the National Infrastructure sectors to meet minimum levels of compliance without having access to an appropriate technical authority with which exceptions or mitigation strategies could be discussed and advice/guidance offered in confidence.

Equally the Competent Authorities might need an appropriate skills source for drafting and management of the CAF as well as to provide independent advice about sectors.

Should an incident occur then appropriate skills should be available to ensure the correct and effective remediation ensuring a resumption of acceptable service levels as soon as possible.

The risks and issues reporting regime would encourage 'early reporting' to prevent incidents occurring and a risk assessment and mitigation skillset would be advantageous.

In other jurisdictions this service is offered through a body known as a CSIRT – Computer Security Incident Response Team.

A CSIRT would provide a pro-active capability by utilising cyber–intelligence, analysis of threats and reports from the National Infrastructure sectors to formulate early warnings and alerts together with mitigation advisories and, in the event of incidents, providing advice, guidance and management to ensure the correct and effective remediation. This function would, therefore, provide a supportive, advisory and preventative function to improve controls and responses, as opposed to a regulator that may result in more formal action, such as a power to impose sanctions where controls could be improved.

PRINCIPLE 8

Compliance Framework

As mentioned in Principle 5 an effective compliance regime would be required to ensure minimum levels of assurance are reached and maintained.

The legislation should include the power to ensure that the sectors of the Island's National Infrastructure notify its CSIRT or Competent Authority of any incident that has a significant impact on the provision of their services. This will enable a picture of potential threats to the Island to be created and enable the CSIRT or Competent Authority to pro-actively advise on protective measures that aim to mitigate and minimise risk. As the legislation proposes to protect the National Infrastructure the Government should be empowered to place conditions or controls on any products or entities believed to present a risk.

The compliance framework should encourage co-operative working practices to ensure the resilience and security of the National Infrastructure. This would be through the ability to promote and share best practices, risks, issues and concerns whilst ensuring an appropriate level of resilience and assurance is maintained in the National Infrastructure and those upon whom it depends to deliver its services.

QUESTIONS

Question 7

Should the threat and incident management capability (CSIRT) support and advise the Competent Authority/regulator in drafting the appropriate minimum levels of compliance as described in Principle 5?

Yes.

Question 7(a)

Bodies referred to as a 'CSIRT' are more usually known as a Cyber Security Incident Response Team, and not a Computer Security Incident Response Team.

Question 8

Who should be responsible for operations of the CSIRT?

- Government
- The designated competent authority **Yes**
- Private sector
- Other (please specify)

Question 9

Do you agree that a competent authority should have the ability to (please indicate)

- Issue enforcement notices **Yes**
- Fine an organisation **Yes**
- Pursue criminal prosecution **Yes**
- None of the above
- Other - **the ability to Investigate**

Question 10

Should organisations that come under the scope of any legislation be required to conduct a self-assessment, outlining their compliance with a Cyber Assurance Framework (CAF)?

Yes.

(if yes) Question 10(a)

What timeframe?

- Quarterly
- Six monthly
- Annually **Yes**

- Other

Question 10(b)

No further comments.

Question 11

In order to assure compliance with a CAF, independent certification measures might be required. Do you agree with this?

Yes.

Question 11(a)

No further comments.

Question 11(b)

How often would these independent certification measures have to occur?

- Annually
- Bi-annual **Yes**
- Triennial
- Other (please state)

Question 12

Should the Competent Authority have the authority to require an independent assessment as and when it sees fit?

Yes.

Question 12(a)

No further comments.

PRINCIPLE 9

Reporting obligations

A risks and reporting regime should be included in legislation affording levels of confidentiality and protection in law whilst also enabling an ability to share details with relevant partners or sectors in the interests of national protection or security.

A risks and issues reporting regime would also afford the ability to require 'early reporting' to prevent incidents occurring or allowing for mitigation steps to be considered. (See Principle 8 – Compliance Framework) creating a both supportive and proactive regime.

QUESTIONS

Question 13

To ensure adequate protection of the National Infrastructure, do you agree that entities that fall under the scope of the legislation should be required to notify of emerging risks, issues or 'near misses.'

Yes.

Question 13(a)

No further comments.

Question 14

If a competent authority with responsibility for implementing the proposed legislation is established should they be the reporting point or should this be reported elsewhere?

- The competent authority **Yes**
- Other (please specify)

Question 15

When an incident occurs, what is an appropriate timeframe for organisations to notify the designated body about an incident?

- Within 24 hours after discovery
- Within 48 hours after discovery
- Within 72 hours after discovery **Yes**
- Within 96 hours after discovery
- Other (please specify)

Question 15(a)

Why do you consider this timeframe appropriate?

As soon as possible after the facts can be established. Or 72 hours for any potential issue under internal investigation to be completed. A status of under investigation if position is unclear.

Question 16

It has been proposed that those entities which fall under the scope of this legislation should only report incidents that are likely to impact the delivery of services. Do you agree with this?

No.

Question 16(a)

(any other comments)

As this would not include fraud, impersonation of websites or persons.

Question 17

In your opinion, which of the following incidents do you feel entities that fall under the scope of this legislation should be compelled to report, noting that these may reflect current incident types that may advance or change in the future?

- Ransomware **Yes**
- Receipt of phishing (email/text/voice) **Attempts no, actual yes**
- Compromise of third party supplier **Yes**
- Impersonation attempts e.g. website impersonation **Yes**
- Fraud attempts such as gift card or invoice fraud **Yes**
- Business email compromise **Yes**
- Malware infection **Yes**
- Intrusion detection **Attempts no, the volume will be massive, actual yes**
- Hacking (incl. Attempts) **Attempts no, actual yes**
- Other (please specify)
  - **Impersonation of key political and government officials**
  - **Threats to the Democratic process (Cyber Threats to Canada's Democratic Process: 2023 update - Canadian Centre for Cyber Security)**
  - **Events that could be reasonably expected to negatively effect the general public. I.e. scams**
  - **Use of Artificial Intelligence for fraudulent or misrepresentation.**

Reporting based on scale of incidents, impact of incidents, number of people affected. Below a minimum level not reported.

PRINCIPLE 10

Transitional Arrangements

When the UK Government introduced the UK Telecom's (Security) Act in 2021, it allowed UK Telecommunications operators a transitional period in which to comply with the changes the legislation now required.

Isle of Man legislation should take a similar approach and grant a transitional period between the legislation being enacted and the deadline for the requirement to evidence compliance.

QUESTIONS

Question 18

Do you agree that transitional periods should be determined by the requirements of each sector and the service delivered?

Yes.

Question 18(a)

Yes, appropriate time should be given to allow transition to a new standard of security compliance and fine for delay in non-compliance proportionate to the organisations' ability to pay to avoid total loss of service.

Consideration should be given to the size of the organisation and its ability to a) complete organisational change within set time frames and b) afford any fines.

If the fines are too great this may result in the organisation deciding not to continue providing that service at all. The incentive to move to a stronger cyber security position needs to be balanced and proportionate, both in fines and risk to national infrastructure.