Isle of Man
Chamber of Commerce

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 tick 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*
- *Transport – including Air, Sea and Road*
- *Financial Services – including banking and market infrastructure*
- *Health – For example, Hospitals, Research and Public Health Laboratories, Primary Care, Mental Health Services, and Social Care*
- *Blue Light Services – For example, Police, Fire & Rescue, and Ambulance*
- *Water – drinking and waste*
- *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*
- *Information Communication Technology (ICT) service management (business to business) Government – public administration, entities of central government*
- *Space – operators of ground based infrastructure that support the provision of space-based services – excluding public electronic communications networks.*
- *Postal and courier services*
- *Waste management*
- *Chemical manufacturing, production, and distribution*
- *Food production, processing and distribution*
- *Manufacturing*
- *Digital providers*
- *Research*
- *Other (Please specify in the text box)*

Isle of Man
Chamber of Commerce

Answer

Other: it is our view that due to both the nature of the Isle of Man and its location (inc. it's reliance on external connectivity, logistic lines and supply of resources) **all** of the above should be considered, of varying degrees, within this legislation and the research underpinning it.

It is also, a key point of concern within the private sector (including the Critical Infrastructure providers) and with individuals (consumers), that in developing this legislation with its associated regulatory framework, the understanding and the impact linked to the implementation thereof would be financially impactful, and thus not overly viable; especially so under the current economic and financial pressures many are facing.

Looking to the individual consumers, such as households and residents, the increase in compliance costs 'would' lead to a potential rise in the cost of services at the point of consumption.

Broadly comparable to other jurisdictions deemed critical national infrastructure, the Isle of Man must take into consideration the key nodes and points of failure, aligned to reliance and protected service delivery agreements from off-island origins of provision; the Island must apply a structured approach with applicable metrics as it considers the differences between the complexity and scale of the infrastructure on the Island against other jurisdictions. It is agreed that the Bill should be based upon relevant legislation from comparable jurisdictions but must also be proportional to the Island's needs and capabilities, as stated within Principle 4 of this consultation.

The Isle of Man must carefully assess which entities are to fall into the scope of the legislation for the proposed bill to be effective. For reference, the UK Governments official definition of Critical National Infrastructure (CNI) is:

'*Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:*

a) *Major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or*
b) *Significant impact on national security, national defence, of the functioning state.'*

Equally, the Isle of Man should consider taking a similar approach to other jurisdictions, such as the UK and EU, when it comes to defining their CNI. Within the UK's NIS regulations 2018 and the EUs NIS1/NIS2 Directives, a tiered approach is taken when defining the entities that fall into scope of the legislation. For example, the UK's NIS regulations split the entities into two categories of Operators of Essential Services (OES) and Digital Service Providers (DSPs). Likewise, the EU splits the entities into the categories of 'Essential Services' and 'Important Entities'. This approach can allow the legislation to apply more stringent requirements on the most critical entities, while less important parts of the national infrastructure can have less rigorous requirements, as touched upon within the Principle 2.

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/no/unsure

Answer

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?

Isle of Man
Chamber of Commerce

Answer

To maintain robust security for the Island's critical infrastructure, the National Infrastructure Security Bill (NISB) should be appropriately and proportionately aligned to the United Kingdom's Security of Network and Information Systems Regulations (NIS Regulations 2018). This is primarily due to the Island's reliance on connectivity and supply from the UK. Consideration should also be given to proposed reforms to the NIS Regulations, which come as a result of a 2022 consultation.

The Isle of Man must ensure that its critical infrastructure security meets the same high standards as those set by the UK. Given that services such as Gas, Electricity, Telecommunication & Connectivity, and Travel (Air and Sea) are interconnected, and in certain instances, reliant on the UK's infrastructure, harmonizing security measures is essential.

Question 2(b)

Any other comments?

Answer

The NIS Regulations 2018 are the UK's application of the EU's Network and Information Systems ('NIS') Directive, tailored to the UK economy. With this, it is reasonable to conclude that the Isle of Man should also take into consideration the EU's NIS and upcoming NIS 2 Directives, which replaced the original NIS Directive and entered into force in January 2023. The NIS 2 Directive is more extensive than the UK NIS regulations, so it is important that the Isle of Man remembers the proportionality of the Directive when taking them into consideration. The NIS2 Directive offers a wider scope of sectors, higher fines and responsibility for supply chain security. A particularly relevant area for the Isle of Man to review in preparation of NISD is the minimum-security measures that all organizations must adhere to under the NIS2 Directive. The EU's 'Critical Entities Resilience' Directive (CER) should also be reviewed in conjunction with the NIS2 Directive.

The Isle of Man should also consider approaches taken in comparable jurisdictions, such as other Crown Dependencies, Malta, Singapore, and Island's within the International Finance Centers (Bahamas, Bermuda, Caribbean Community (CARICOM), etc). This is felt necessary as these nation states are largely comparable in economic delivery of services and also in size, scale and other essential criterion.

Isle of Man
Chamber of Commerce

For example, Jersey has implemented a 'CSRIT' as proposed within this consultation. Jersey's CSIRT is referred to as the 'Cyber Emergency Response Team' or 'CERT' which operates at arm's length from the Jersey Government. A 2022 'Consultation on proposed Cyber Defense legislation' provides insight into how Jersey approaches cyber security.

Singapore has established 'The Cyber Security Agency of Singapore' (CSA), in which the 'SingCERT', or Singapore Cyber Emergency Response Team' operates. Appropriate legislation to review would be the Cyber Security Act 2018, which saw the appointment of the Commissioner of Cyber Security, along with its respective authoritative powers, and other guidelines for organizations.

Malta is in the process of transposing the EU's CER and NIS2 Directives into Maltese law. The 'Transposition of Directive 2016/1148' already in place within Malta establishes necessary protective cyber security measures for Maltese critical infrastructure. The Directive established the Critical Information Infrastructure Protection (CIIP) Unit as their competent authority and Single Point of Contact (SPOC). The CIIP unit sits within Malta's Critical Infrastructure Protection (CIP) Directorate, along with Malta's CSIRT (CSIRTMalta).

Other comparable jurisdictions such as those in Caribbean area do not yet have relevant legislation to review, although approaches can be taken into account, such as the Bermuda Cybersecurity Strategy 2022, Bahamas National Cybersecurity Project, and the Cayman Island Monetary Authority guidance on Cybersecurity for Regulated Entities.

Please see the below for more information:

- Jerseys 2022 'Consultation on proposed Cyber Defense legislation': https://www.gov.je/SiteCollectionDocuments/Government%20and%20administration/Consultation%20on%20proposed%20cyber%20defence%20legislation.pdf
- Singapore CSA: https://www.csa.gov.sg/
- SingCERT: https://www.csa.gov.sg/Explore/who-we-are/our-identity/about-singcert
- Malta's CIP Directorate: https://maltacip.gov.mt/en/cip_structure/pages/cip-directorate.aspx

Isle of Man
Chamber of Commerce

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.

Answer

The Isle of Man should model their CAF upon the UK National Cyber Security Centre's (NCSC) CAF. The NCSC CAF was developed to meet an appropriate set of requirements, including compatibility with existing cyber security guidance / standards; existing in a common, sector-agnostic version; being extensible to accommodate sector-specific elements as required; and being as straightforward and cost-effect to apply as possible. These requirements are aligned with principle 5 of this consultation, 'Any CAF would need to be flexible to meet sector specific needs and risks.' The requirements, along with the comprehensive assessment methodology, makes the NCSC's CAF an appropriate framework for the Isle of Man to baseline against.

Chapter IV of the NIS2 Directive, 'Cybersecurity risk-management measures and reporting obligations', should also be reviewed in the development of a CAF. Chapter IV lists technical, operational and organisations measures that are required under the directive, including 30+ documents that must be written.

Other appropriate standards that should be reviewed in the preparation of instructions for the legislation are those referenced by the UK ICO, who is the regulator for Digital Service Providers under the NIS regulations, and the European Union Agency for Cybersecurity (ENISA). These standards include ISO/IEC 27001; ISO/IEC 22301; ISA/IEC 62443 and NIST CSF. CREST also has several pen-test frameworks which should be reviewed in the preparation of the legislation, including CBEST, GBEST and TBEST.

Please see the below for more information:

- NCSC CAF Guidance: https://www.ncsc.gov.uk/collection/caf
- ICO Guidance: https://ico.org.uk/for-organisations/the-guide-to-nis/security-requirements/
- ENISA Minimum Security Measures against appropriate standards: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/minimum-security-measures-for-operators-of-essentials-services

- CREST (CBEST, GBEST and TBEST): https://www.crest-approved.org/membership/government-regulators/

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*
- *Existing regulator where appropriate*
- *Other (please specify)*

Answer

The current governmental construct within the Isle of Man has no clear entity to enable an authority to either be embedded within or remit expanded to include. Due to the nature of the activity under this Bill, it is advised that a competent body be formed, such as via a new arm's Length body/organisation i.e. Office of Infrastructure Security. The new organisation should have enough competence, influence and ability to operate with credibility to operate as required.

Question 5

Who should provide oversight/monitoring for a competent authority

- *Government Department (please specify)*
- *Board (public sector)*
- *Board (public and private sector)*
- *Board (private sector)*

Answer

Government Department and Board (public and private sector)

Question 6

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

Isle of Man
Chamber of Commerce

Answer

If the authority was to sit within a newly established arm's length body/organisation, provision of oversight/monitoring should be the responsibility of a Government Entity, in particular the Department for Home Affairs. The DHA aims to '*provide effective services for the safety, protection and security of the Islands residents and businesses'*, which security of the national infrastructure falls scope to for both physical and technical security measures.

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/no/unsure

Answer

Yes

Question 7(a)

(any other comments)

Answer

Similar approaches are seen with comparable jurisdictions such as the UK and Jersey. The Isle of Man should analyse these comparable jurisdictions compliance levels and apply appropriate scaled and baselined protocols accordingly. be follow for best practice.

Regulation 5 of the NIS Regulations 2018 assigns the CSIRT with functions, which include promoting the adoption and use of common or standard practices for incident and risk handling procedures, as well as incident, risk and information classification schemes. Notably, the UKs NCSC, which developed the UK's CAF, serves as the UK's CSIRT and technical authority for addressing cyber threats.

Please see the below for more information:

- NIS Regulations 2018: https://www.legislation.gov.uk/uksi/2018/506/2023-05-03
- About NCSC: https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

Question 8

Who should be responsible for operations of the CSIRT?

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

Answer

To promote an open and collaborative relationship between the CSIRT and the Authority, the competent Authority should be responsible for the operations of the CSIRT. This will enhance the competent authority's understanding and oversight of the cyber landscape which it regulates. Regular communication between the CSIRT and the Authority can also be beneficial when considering the development and maintenance of the CAF, as the CSIRT will have a better understanding of the risk horizon than the Authority will.

The Island should also consider looking to the UK system to garner support and operational delivery due to the close reliance of, connectivity and provision to the UK across near all of the Island's national infrastructure provisions.

Question 9

- *Do you agree that a competent authority should have the ability to (please tick)*
- *Issue enforcement notices*
- *Fine an organisation*
- *Pursue criminal prosecution*
- *None of the above*
- *Other*

Answer

All the above should be considered, dependent on the authority being a new organisation with the appropriate applicable powers. If the current construct within the Isle of Man Government is given the authority, the activities, actions, abilities and competence of the

authority should be closely reviewed by an independent panel composing both public and private sector experts.

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/no/unsure

Answer

Yes

Question 10(a)

What timeframe?

- *Quarterly*
- *Six monthly*
- *Annually*
- *Other*

Answer

Annually

Question 10(b)

(Any other comments)

Answer

Self-assessments should be required to be submitted annually, however, in the event of significant changes to an organization's cyber infrastructure, provision, etc. then recertification should be required. Rationale behind recertification, is that it provides both the authority, and the organisation with a better understanding of the threats and vulnerabilities within their infrastructure, giving the organisation an opportunity to put in mitigating factors, rather than wait for recertification of a cycle basis.

Isle of Man
Chamber of Commerce

Question 11

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

Yes/no/unsure

Answer

Yes

Question 11(a)

(any other comments)

Answer

Independent third parties following a level of accreditation by the authority should be able to support the critical infrastructure organisations in attaining alignment / compliance through the CAF.

A process similar to that of the GFSC programme aligned to NIST CSF.

Question 11(b)

How often would these independent certification measures have to occur?

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

Answer

Full detailed (re-)certification measures should occur biennially (every other year/2 years). As with self-assessments, recertification should have to take place upon significant changes occurring within the entity's infrastructure. An annual high-level self-certification, and or statement of compliance, should be required from each registered entity to the authority.

Question 12

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

Yes/no/unsure

Answer

No

Question 12(a)

(any other comments)

Rather than when it sees fit, the Competent Authority should have the authority to require an independent assessment based upon pre-defined criteria. This pre-defined criterion should be based upon and aligned to agreed SLA's / KPI's / CSFs/ CRFs relative to the sector and take the form of a decision matrix. Upon the relevant criteria being met, only then should the Competent Authority be able to use its authoritative powers and enforce an independent assessment.

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/no/unsure/no views

Answer

Yes

Question 13(a)

(any other comments)

Answer

Entities that fall under scope of the legislation should be required to notify based upon pre-defined criteria which is relevant to their sectors. This pre-defined criterion should be

based upon and aligned to agreed SLA's / KPI's / CSFs/ CRFs relative to the sector and take the form of a decision matrix. Upon the relevant criteria met, the entity would then be required to notify of emerging risks, issues or 'near misses.

The use of a matrix would ensure that only appropriate risks/issues are being reported. This would ensure that an organisation does not have to invest too much resource into reporting all events and helps combat the CSIRT and / or Competent Authority becoming overburdened from a potential continual influx of reporting.

In addition, it should be considered that if the 'authority' were to be come aware of any significant risks and or issue to the Island's critical infrastructure, it should have the authority to seek the sectors response to that risk or issue – such as, confirmation that appropriate measures are in place to offset, mitigate, manage or transfer any raised risk, and or procedures, policies and protocols for the management of the issue.

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*
- *Other (please specify)*

Answer

The Competent Authority should be the reporting point. This aligns with both the NIS Regulations 2018, and the NIS 2 Directive (which also allows reporting to the CSIRT as appropriate). Ultimately, the Isle of Man should use the NIS Regulations as the baseline for the NISB, therefore the reporting point should be the competent authority.

Isle of Man
Chamber of Commerce

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*
- *Within 96 hours after discovery*
- *Other (please specify)*

Answer

OTHER:

Timeframes should be scalable and dependent on the severity of the incident and the respective infrastructure area, but in all cases should be within 72 hours after discovery. It should be encouraged to report an incident without undue delay across all sectors, with the deadline being dependent on severity and sector.

Services deemed to be most critical to the Island should have to notify the designated body on a quicker basis than those who offer essential services but are not crucial to the island's survival. E.g., Significant Incidents within the Energy sector must be reported within 24 hours after discovery, whereas Digital Providers must report incidents within 72 hours after discovery.

Question 15(a)

Why do you consider this timeframe appropriate?

Answer

The UK NIS Regulations 2018 requires for Operators of Essential Services (OES's) to notify the designated competent authority about any incident which has a significant impact of the service it provides without undue delay, and in any event no later than 72 hours after the operator is aware that the incident has occurred (Regulation 11 (1)-(3)).

Likewise, the EUs NIS 2 Directive requires that essential and important entities notify, without undue delay its CSIRT or Competent Authority (as applicable) of any significant event. It is further specified that within 24 hours of becoming aware of the significant

incident, an early warning shall be submitted, which indicates whether the incident is suspected of being caused by unlawful or malicious acts or could have cross-border impact. Within 72 hours of becoming aware of the incident, an incident notification must be provided which updates the suspicion status and indicates an initial assessment of the incident, including severity and impact. (Article 23)

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?

Yes / No / Unsure

Answer

No

Question 16(a)

(any other comments)

Answer

More factors need to be considered, rather than just the impact to the delivery of services. Reports should be based upon the severity of the incident, and the sector in which the incident occurs. Within comparable jurisdictions, other aspects are considered, as well as the impact to the delivery of services.

Within the EU's NIS 2 Directive, any incident that has a significant impact on the provision of their services must be notified to the CSIRT / Authority (As applicable). Under the directive, an incident considered to be significant if: it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned; or it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

Likewise, in the UKs NIS Regulations 2018, it is states that an OES must report any incident which has a significant impact on the continuity of the essential service which the OES provides. To determine the significance of the impact of an incident an OES must have

regard to: the number of users affected by the disruption of the service; the duration of the incident; and the geographical area affected by the incident.

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*
- *Receipt of phishing (email/text/voice)*
- *Compromise of third party supplier Impersonation attempts e.g website impersonation*
- *Fraud attempts such as gift card or invoice fraud*
- *Business email compromise*
- *Malware infection*
- *Intrusion detection*
- *Hacking (incl. Attempts)*
- *Other (Please specify in the text box)*

Answer

All the above, with the exception that phishing/malware/intrusion/hacking should only be reported if the organisation has fallen victim to it and the attempt has been successful (albeit contained/remedied). Additionally, breaches to and or attempts to compromise the physical security measures adopted by the sector entity should also fall under scope, including infiltration, intrusion, theft, and damage.

Isle of Man
Chamber of Commerce

Question 18

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

Yes/No/Unsure

Answer

Yes

Question 18(a)

(any other comments)

Answer

Periods should be determined based upon the criticality of the respective sector / infrastructure area. i.e., Sectors deemed to be the most critical to implement requirements earlier than less essential services. A scaled and incremental approach to implementation should be considered based upon known risks and issues to the sector and the relative 'scoring' on the sector risk/issue mapping activity undertaken.

Submission made by Isle of Man Chamber of Commerce Digital Forum