



Office of Cyber-Security
& Information Assurance
Oik san Shickyrys Lectraneagh as Sauchys Fysseree



Cyber Security Centre
for the Isle of Man

National Infrastructure Security Bill (NISB)

Consultation

01/12/2025 - 09/01/2026

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 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.

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 providers, some will be more critical to our daily lives and the Isle of Man economy than others. Equally some will be larger than others.

To explain this further we've created a handy guide to the proposed bill, and we encourage you to read.

[NISB Reference Guide](#)

Previous Consultations

As part of the [National Cyber-Security Strategy 2022-27](#) we are committed to developing a resilient and responsive digital island. A core tenant of this is insuring our critical national infrastructure remains resilient in the face of a cyber-attack.

To that end, In February - March 2024 we consulted on the policy principles of the proposed bill. This consultation served to explore how a potential bill would look and whether it was necessary to ensure national security.

Feedback gave us a mandate to proceed with drafting the bill and results from the previous consultation can be found below.

[NISB Consultation February 2024](#)

What Happens Next?

Following the consultation, the results will be reviewed.

Where appropriate, we will liaise further with respondents.

A consultation summary will be produced and made available on the Consultation Hub.

The Consultation period will end on the 9th of January 2026.

Reasonable Adjustments and Alternative Formats

The Department is committed to equal opportunities and our aim is to make our documents easy to use and accessible to all.

We will take steps to accommodate any reasonable adjustments and provide such assistance as you may reasonably require to enable you to access or reply to this consultation.

If you would like to receive this document in another format or need assistance with accessing or replying to this consultation, please email OCSIA-Secretariat@gov.im or telephone

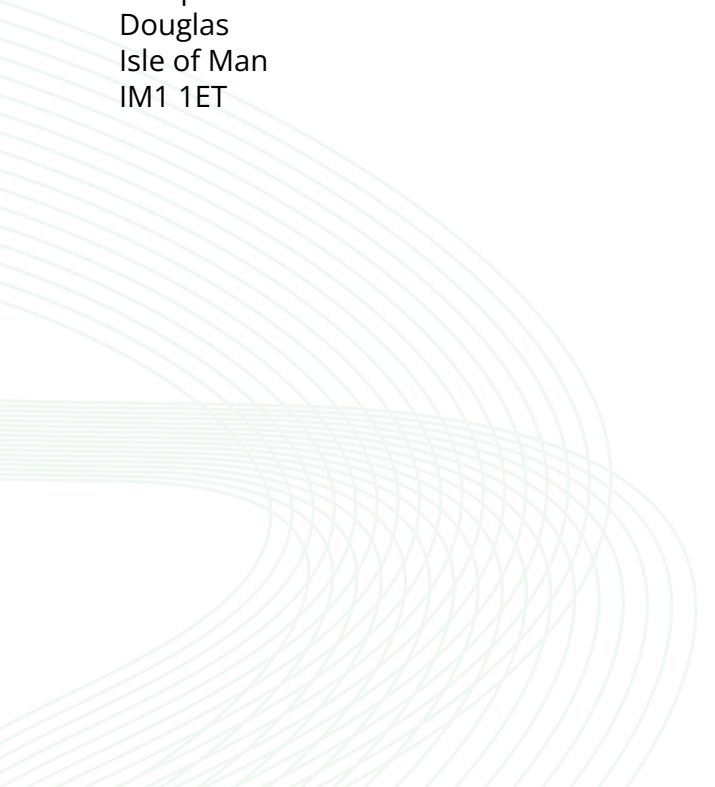
T: +44 1624 685557.

Responding to this Consultation and Questions

You can respond to this consultation online by clicking on the 'Online Survey' link.

Alternatively you can download a paper version of this consultation in the 'Related' section below and email it to OCSIA-Secretariat@gov.im or sent it to the below address.

NISB Response OCSIA
Second Floor 27-29
Prospect Hill
Douglas
Isle of Man
IM1 1ET



About You

Which option best describes your interest in responding to this consultation?

- ☐ Member of public
- ☐ Isle of Man Government
- ☐ Business owner or Stakeholder
- ☐ Member of Tynwald
- ☐ Other (please specify)

Other:

Are you responding on behalf of an organisation or industry?

- ☐ Yes
- ☐ No

Organisation / industry: _____

Number of people or organisations represented: _____

May we publish your response?

- ☐ Yes, you can publish my response in full
- ☐ Yes, you may publish my response anonymously
- ☐ No, please do not publish my response

More Information:

Publish in full – your organisation name, or the industry you represent, along with full answers may be published on the hub (your email will not be published)

Publish anonymously – only your responses may be published on the hub (your organisation name, or the industry you represent, and email will not be published)

Do not publish – nothing will be published publicly on the hub (your response will only be part of a larger summary response document)

Section 1: Fundamental Principles

Understanding the scope and implications of the National Infrastructure Security Bill begins with clarity on three foundational concepts: national infrastructure, critical national infrastructure, and security incidents. These definitions underpin the regulatory framework and inform the duties, powers, and protections established throughout the legislation.

National Infrastructure

The Bill defines national infrastructure broadly to encompass the essential components that support the functioning of the Isle of Man and its economy. Specifically:

“national infrastructure’ means the facilities, systems, assets (both physical and digital), sites, information, people, networks and processes necessary for the functioning of the Island and its economy.” (Clause 3 1(a))

This inclusive definition ensures that both tangible and intangible elements—ranging from physical utilities to digital networks and human expertise—are recognised as integral to national resilience.

Critical National Infrastructure (CNI)

Within the broader category of national infrastructure, the Bill identifies a subset deemed critical due to the potential severity of impact if disrupted:

“the ‘critical national infrastructure’ comprises those parts of the national infrastructure the disruption of which would have a severe and significant impact on the Island’s national security, economic stability, public health or safety.” (Clause 3 (1b))

Security Incidents

The concept of a security incident is central to the Bill’s risk management and response mechanisms. It is defined as:

“anything that compromises the availability, performance or functionality of [national] infrastructure; or any unauthorised access to, interference with or exploitation of that infrastructure or anything that enables such access, interference or exploitation.” (Clause 4)

For public electronic communications networks or services, the definition is extended to include breaches of confidentiality, data loss or alteration, and incidents that may lead to further security compromises.

Importantly, the Bill also recognises potential threats:

“A security incident includes anything that has the potential to have any of the effects referred to in subsection (1).” (Clause 4(2))

Section 1: Questions

Q1. Do you find the definitions of “national infrastructure” and “critical national infrastructure” in Clause 3(1) clear and sufficient for identifying relevant sectors and assets?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Q2. Is the definition of a “security incident” in Clause 4 comprehensive and appropriate?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Section 2: Provider Classification and Registration

The National Infrastructure Security Bill introduces a tiered classification system for providers involved in the national infrastructure. These classifications—essential registered providers, important registered providers, and unclassified register providers—determine the level of regulatory oversight and the nature of the obligations imposed under the Act.

Entity Classifications

Under Clause 22, providers are categorised as follows:

“A person who, in accordance with the Schedule, is categorised as an essential, important or unclassified provider must —

- (a) register as such a provider; and*
- (b) do so by entering the prescribed details (under regulations referred to in section 10) in the register.”*

The classification of a provider is determined by the Schedule to the Act, which outlines the sectors and sub-sectors of the national infrastructure. Essential entities are those whose operations are deemed vital to the functioning of critical national infrastructure, while important entities play a significant but less central role. Providers that do not fall into either category but still provide relevant goods, services, or facilities must still register and comply with baseline standards.

Registration Requirements

All providers falling within the scope of the Act must be entered into a central register maintained by the responsible authority. As per Clause 9 (2a):

“A responsible authority must establish and maintain a register of persons who are required to be entered in it as registered providers.”

The responsible authority determines the specific details required for registration and may also define categories of registration. The Department of Home Affairs may further regulate the information to be included in each providers entry.

Ongoing Registration Conditions

Once registered, providers are subject to ongoing compliance obligations. Clause 11 provides that:

“The Department may determine different ongoing registration conditions for different categories of registration or for different registered providers or groups of provider... The Department must ensure that ongoing registration conditions are proportionate to its assessment of the risk posed to the critical national infrastructure by the provider in question.”

These conditions may vary depending on the classification of the provider and the nature of its operations. The responsible authority is also empowered to revise these conditions and must consult relevant stakeholders where appropriate.

Section 2: Questions

Q3. Are the three classifications of essential, important, and unclassified enough to make regulations in respect of an assurance framework?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Q4. Do the registration requirements in Clause 10 and the ongoing conditions in Clause 11 provide sufficient clarity and flexibility?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Q5. Are providers are appropriately allocated in schedule?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Section 3: Resilience and Cybersecurity Standards

The National Infrastructure Security Bill establishes a structured division of responsibilities between the Department of Home Affairs (referred to as “the Department”) and the responsible authorities in relation to resilience and cybersecurity standards for the national infrastructure.

Role of the Department

The Department holds the primary authority for setting minimum standards. Clause 12 provides that:

*“The Department may, by regulations, make provision in respect of minimum standards in relation to—
(a) critical national infrastructure resilience; and
(b) cyber security.”*

These regulations may address the content of the standards, who must comply, penalties for non-compliance, and how the standards are to be revised and published. This centralised role ensures consistency across sectors while allowing for sector-specific adaptations.

Role of Responsible Authorities

While the Department sets the overarching standards, responsible authorities are responsible for sector-specific implementation and oversight. They may issue guidance on how providers should meet these standards and ensure compliance through registration and monitoring mechanisms. Clause 9 (3) empowers responsible authorities to:

*“issue guidance about—
(a) cyber security standards or any similar standards;
(b) how it proposes to exercise its powers, and perform its functions, under this Act.”*

This allows for tailored regulatory approaches that reflect the operational realities of different sectors within the national infrastructure.

Consultation and Publication Requirements

Clause 12 also embeds a requirement for collaborative governance and transparency:

“(3) Before making regulations under this section the Department must consult the technical authority.”

This ensures that technical expertise informs policy and that the standards are both practical and proportionate. Furthermore, the Department is expected to publish the standards, including any revisions, to ensure accessibility and accountability.

Section 3: Questions

Q6. Is the division of responsibilities between the Department (Clause 12) and responsible authorities (Clause 7 & 9) for setting resilience and cybersecurity standards clear and workable?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Q7. Are the consultation and publication requirements in Clause 12(2)–(3) sufficient to ensure transparency and stakeholder engagement?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Section 4: Responsibilities of the Technical Authority

This section outlines the core responsibilities of the Technical Authority in supporting the security and resilience of the Isle of Man's national infrastructure, as set out in clauses 14-21. The Technical Authority, designated as the Cyber Security Centre for the Isle of Man, plays a pivotal role in monitoring, advising, and coordinating responses to cyber threats and vulnerabilities.

Key responsibilities include:

- Advising responsible authorities and registered providers on technical matters related to infrastructure security.
- Conducting proactive scanning and assessments of network and information systems.
- Coordinating incident response and maintaining situational awareness of global cyber threats.
- Acting as a central point of contact for infrastructure-related cybersecurity matters.
- Reporting to the Department on security incidents and emerging risks.
- Providing technical support, guidance and review on behalf of the responsible authorities when requested.

The Technical Authority is independent and required by law to maintain confidentiality.

These responsibilities ensure that the Technical Authority remains a trusted partner in safeguarding the Island's infrastructure.



Section 4: Questions

Q8. Are the responsibilities of the Technical Authority clearly defined and appropriate?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Q9. Does the role of the Technical Authority provide sufficient support to registered providers?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Q10. Are there additional functions the Technical Authority should undertake?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Section 5: Incident Notification and Reporting

The Bill sets out a structured timeline for entities to notify and report security incidents to the Technical Authority. These timeframes are designed to ensure timely awareness and response to threats affecting the national infrastructure.

Under Clause 30(2), providers must:

“notify the Authority no later than 24 hours after it becomes aware that the incident has occurred, or the potential threat arises.”

This 24-hour window ensures that the Technical Authority is alerted promptly to any incident that may have a significant impact on the goods, services, or facilities provided to the critical national infrastructure.

Following the initial notification, Clause 31 requires two further reports:

- Interim Report: “no later than 72 hours after the security incident occurred, or as the case may be, the potential threat arose;”
- Final Report: “no later than one month after the incident was dealt with, or as the case may be, the potential threat arose.”

These reports are intended to provide a fuller picture of the incident’s nature, impact, and resolution, supporting both immediate response and long-term resilience planning.

Definition and Threshold of “Significant Impact”

The obligation to notify the Technical Authority is triggered when an incident is considered to have a “significant impact”. Clause 30(3) outlines the criteria for assessing significance:

“In determining... whether the effect that an incident has, or would have, on the critical national infrastructure is significant, the following matters in particular are to be taken into account—
(a) the length of the period during which the operation of the impacted service is, or would be, affected;
(b) the number of persons who use the impacted service that are, or would be, affected;
(c) the size and location of the geographical area... affected;
(d) the extent to which activities of persons who use the impacted service are, or would be, affected.”

This multi-factor test ensures that both the scale and severity of an incident are considered, allowing for proportionate responses and prioritisation of resources.

Section 5: Questions

Q11. Are the timeframes for incident notification and reporting in Clauses 31–32 (24-hour notification, 72-hour interim, one-month final) appropriate and achievable?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Q12. Are the thresholds for what constitutes a “significant impact” in Clause 31(3) clear?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Section 6: Compliance and Oversight

The Bill grants responsible authorities robust powers to monitor and assess whether providers are complying with their obligations under the Act. Clause 35 provides the foundation for this oversight:

“A responsible authority may carry out, or arrange for another person to carry out, an assessment of whether that provider is complying or has complied with a security duty imposed on the registered provider.”

To facilitate these assessments, Clause 36 empowers authorities to issue assessment notices, which may require entities to undertake a range of actions, including:

“(a) carry out specified tests...”

“(b) make arrangements for another person to carry out tests...”

“(d) permit an authorised person to enter specified premises;

“(g) direct an authorised person to documents...”

“(k) provide an authorised person with an explanation of such documents, information, equipment or material.”

These notices must specify the timeframe for compliance and include information about the consequences of non-compliance and the right of appeal.

In addition, Clause 60 introduces inspection notices, which may be issued where the Department has directed a responsible authority to monitor compliance with a Designated Vendor Direction (DVD). These notices can require providers to:

“make available for interview a specified number of persons...”

permit an authorised person to observe any operation...

comply with a request for a copy of documents...”

Inspection notices must provide at least 28 days' notice and cannot require entry into domestic premises or the disclosure of legally privileged information.

Enforcement Mechanisms

Where non-compliance is suspected, the Bill provides a structured enforcement process. Clause 39 allows a responsible authority to issue a notification of contravention, which:

“sets out the determination made by the authority;

specifies the duty in respect of which that determination has been made;

specifies the period during which the provider in question has an opportunity to make representations;

specifies the steps that the authority think should be taken...

specifies any penalty which the responsible authority is minded to impose.”

The authority may also propose interim steps under Clause 42 where there is an imminent risk of a security incident, and may issue a direction under Clause 43 requiring those steps to be taken.

These enforcement powers are complemented by civil remedies, including injunctions and specific performance, ensuring that authorities can act swiftly and proportionately to protect the national infrastructure.

Section 6: Compliance and Oversight

Q13. Are the powers of responsible authorities to assess compliance under Clauses 35–36 (including assessment notices and inspections) proportionate and clearly described?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Q14. Are the enforcement mechanisms in Clauses 39–43 effective and proportionate?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Section 7: DVNs, DVDs and Infrastructure Protection Orders

Designated Vendor Notices (DVNs)

A Designated Vendor Notice (DVN) is a formal designation issued by the Department to identify a vendor whose goods, services, or facilities may pose a risk to national security. As per Clause 46:

“The Department may issue a notice (‘a DVN’) designating a person (‘the designated vendor’)... only if the Department considers that the notice is necessary in the interests of national security.”

The Department may consider a wide range of factors, including the nature and reliability of the vendor’s products, their use in the Island or abroad, and the vendor’s ownership or control structure. A DVN must specify the reasons for designation unless doing so would be contrary to national security (Clause 46(5)–(6)).

Before issuing a DVN, the Department must consult the proposed vendor *“so far as it is reasonably practicable to do so”* (Clause 47(1)), unless such consultation would be contrary to the interest of national security (Clause 47(2)).

Designated Vendor Directions (DVDs)

A Designated Vendor Direction (DVD) is a regulatory instrument issued to a provider that uses goods or services from a designated vendor. Clause 50 states:

*“The Department may give a direction... to a registered provider... only if it considers that—
(a) it is necessary for the protection of the critical national infrastructure or in the interests of national security or both; and
(b) the requirements imposed... are proportionate to what is sought to be achieved.”*

DVDs may impose a range of requirements, including prohibiting the use of certain goods, mandating their removal, or restricting how they are used (Clause 51). The Department must consult affected entities and vendors before issuing a DVD, unless this would be contrary to national security (Clause 52).

Variation and Revocation

Both DVNs and DVDs are subject to ongoing review and may be varied or revoked. For DVNs, Clause 48 provides:

*“The Department may—
(a) vary a DVN;
(b) revoke a DVN (whether wholly or in part).”*

Variation is only permitted if it remains necessary in the interests of national security. Similar provisions apply to DVDs under Clause 54, which also requires that any variation be proportionate and necessary.

In both cases, the Department must consult affected parties where practicable and notify them of the changes, including the reasons and effective date—unless doing so would compromise national security (Clauses 48(5)–(8) and 55(3)–(5)).

Section 7: DVNs, DVDs and Infrastructure Protection Orders

Infrastructure Protection Orders

The bill introduces the concept of Infrastructure Protection Orders (IPOs) as a complementary mechanism to Designated Vendor Notices (DVNs) and Designated Vendor Directions (DVDs). Clauses 68–71 set out the statutory basis for IPOs, detailing their scope, conditions for issuance, and procedural safeguards. IPOs may be issued where a serious threat or risk to essential infrastructure is identified and cannot be mitigated through existing measures.

IPOs enable the Department to mandate specific actions by registered providers to protect critical infrastructure assets. These actions may include operational changes, enhanced monitoring, or temporary restrictions on the use of certain technologies.

The integration of IPOs with the DVN/DVD framework ensures a comprehensive approach to infrastructure protection, allowing for both vendor-specific and infrastructure-specific interventions.

IPOs are subject to review and must be published with clear explanations of their scope and duration.



Section 7: Questions

Q15. Are the criteria for issuing DVNs and DVDs under Clauses 47–49 and 57–59 clear and justified?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Q16. Is the process for consultation, variation, and revocation of DVNs and DVDs (Clauses 47–49, 52–55 & 57) sufficiently transparent and accountable?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Q17. Do Infrastructure Protection Orders (Clauses 68–71) provide a necessary complement to DVNs and DVDs?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Section 7: Compliance and Oversight

Q18. Are the criteria for issuing IPOs sufficiently clear and justified?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Q19. Should IPOs be subject to additional safeguards or oversight mechanisms?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Section 8: Information Requests and Non-Disclosure

The Bill grants the Department significant powers to obtain information necessary for the exercise of its functions under Clauses 46–63 and 68–71. Clause 72(1) states:

“The Department may require a person... to provide it with such information as it may reasonably require for the purpose of exercising its functions under sections 46 to 63 and 68 to 71.”

This includes not only existing information but also the power to compel individuals or providers to generate, collect, retain, or analyse data (Clause 72(3)). The scope of information includes details about the use or proposed use of goods, services, or facilities, and the operation or development of public electronic communications networks (Clause 72(4)).

Safeguards and Proportionality

To ensure these powers are exercised responsibly, Clause 73 introduces important safeguards. The Department must issue a formal notice describing the required information and the reasons for the request (Clause 73(2)–(3)). However, this requirement may be waived if providing reasons would be contrary to national security (Clause 73(4)).

Crucially, Clause 73(5)–(6) provides that:

“The Department is not to require the provision of information... except where the making of a demand... is proportionate to the use to which the information is to be put...”

Additionally, Clause 73(7) protects legal professional privilege, ensuring that no person is required to disclose privileged information.

Non-Disclosure Provisions

To protect sensitive information, the Bill includes robust non-disclosure provisions. Clause 67 allows the Department to prohibit disclosure of the contents or existence of certain notices or directions:

“The Department may require a registered provider or a designated vendor who has been sent a copy of a DVD not to disclose to any other person, without its permission, the contents of the DVD or a part of it specified by the Department.” (Clause 67(1))

This applies equally to DVNs, notifications of contravention, confirmation decisions, and urgent enforcement directions. The Department may only impose such a requirement if it considers that disclosure would be contrary to the interests of national security (Clause 67(8)).

Enforcement of Non-Disclosure

Clause 67 extends the enforcement framework to non-disclosure obligations. It applies the same enforcement mechanisms used for DVDs.

Section 8: Questions

Q20. Are the powers to request information under Clauses 72–74 proportionate and clearly limited by safeguards in Clause 73?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Q21. Are the non-disclosure provisions in Clause 67 (including restrictions on sharing the contents of certain notices or directions) clear, proportionate, and necessary for national security?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Section 9: Fines and Penalties

The National Infrastructure Security Bill introduces a proportionate enforcement framework to encourage compliance and deter non-compliance among providers operating within the Island's Critical National Infrastructure (CNI). The aim is not punitive, but to ensure that minimum standards of resilience and cybersecurity are consistently met across sectors.

Civil Penalties and Enforcement Powers

Where a provider fails to meet its obligations under the Act—such as registration, reporting, or adherence to resilience standards—responsible authorities may issue a notification of contravention. This sets out the nature of the breach, the steps required to remedy it, and any proposed penalties. Under Section 80, penalties may include:

- Daily fines for continuing contraventions after the compliance period has expired.
- Penalties for specific breaches, proportionate to severity and impact.
- Urgent enforcement directions where there is an imminent risk to national security or critical infrastructure.

“In the case of a notification under section 62 which relates to a contravention of a requirement imposed by a DVD under section 50—

- (a) any penalty may not exceed 10 per cent of the turnover of the person's relevant business for the relevant period, subject to paragraph (b); and*
- (b) any penalty specified under section 63(9), may not exceed £100,000 per day.” (Clause 80 (4)).*

Dispute Resolution and Appeals

Where a provider disputes a finding of non-compliance or the imposition of a penalty, the Bill provides for appeal mechanisms through tribunals or the Courts. This ensures fairness and transparency in enforcement decisions (Clause 84).

Encouraging Compliance

The Bill recognises that not all providers have equal resources or risk profiles. The enforcement framework is designed to be proportionate, considering the size, sector, and criticality of the entity. Responsible authorities are encouraged to work collaboratively with providers to resolve issues before formal penalties are considered.

High-Risk Categories and National Security

Providers operating in high-risk categories—such as those using goods or services from designated vendors—may be subject to enhanced scrutiny and enforcement. These measures are intended to mitigate unacceptable risks to national security and ensure that vulnerabilities are addressed promptly.

Section 9: Questions

Q22. Do you agree that the proposed fines and penalties are proportionate to the risks posed by non-compliance?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Q23. Is the distinction between civil penalties and enforcement actions (e.g. urgent directions, tribunal appeals) clear and appropriate?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Q24. Do you support the use of higher penalties for breaches involving designated vendors or national security risks?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Section 9: Questions

Q25. Does the Bill strike the right balance between encouraging compliance and enabling enforcement?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Q26. Are there any additional safeguards or considerations you believe should be included in the enforcement framework?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Section 10: Codes of Practice and Assurance Frameworks

The Bill recognises that clear, practical guidance is essential for ensuring consistent compliance across sectors. To this end, it empowers the Department to issue codes of practice and establish assurance frameworks that support providers in meeting their obligations.

Clause 75 provides that:

“The Department may—

(a) issue a code of practice giving guidance as to the measures to be taken under sections 28 and 29 by a registered provider;

(b) revise a code of practice issued under this section and issue the code as revised;

(c) withdraw a code issued under this section.”

These codes are intended to guide entities in implementing appropriate security and risk-management measures, including incident response and resilience planning. While not legally binding, they carry significant weight. Clause 78(2)–(3) states that:

“In any legal proceedings... the court or tribunal must take into account a provision of a code of practice... A responsible authority must take into account a provision of a code of practice in determining any question arising in connection with the carrying out by it of a relevant function.”

In parallel, Clause 23 requires the Department to establish assurance frameworks for essential and important entities. These frameworks may include:

“security and risk assessments and certifications; business continuity plans; independent certification of compliance; and penalties for non-compliance.”

This structured approach ensures that providers are not only aware of their duties but also supported in demonstrating and maintaining compliance.

Procedures for Issuing, Revising, and Withdrawing Codes

The Bill sets out a transparent and consultative process for managing codes of practice. Clause 76(1) requires that before issuing or revising a code, the Department must:

“publish a draft...

consult the responsible authorities, registered providers to whom the draft would apply and such other persons as the Department considers appropriate about the draft.”

Following consultation, the Department must lay the draft before Tynwald and publish the final version (Clause 76(2)–(3)). Codes come into force upon publication unless a different commencement time is specified (Clause 76(4)).

Withdrawal of a code is similarly governed by a formal process. Clause 77 requires the Department to:

“(a) publish notice of the proposal to withdraw the code; and

(b) consult the responsible authorities, affected providers, and other relevant persons.”

Once withdrawn, a notice must be published and laid before Tynwald (Clause 77(2)), with the withdrawal taking effect upon publication unless otherwise stated.

Section 10: Questions

Q27. Is the role of codes of practice and assurance frameworks (Clauses 23, 75–79) in supporting compliance clearly articulated?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Q28. Are the procedures for issuing, revising, and withdrawing codes of practice (Clauses 75–77) sufficiently robust?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Section 11: Reporting and Monitoring

Responsible authorities are required to submit regular reports to the Department to support policy development and ensure oversight of the national infrastructure's security. Clause 13 mandates the preparation of a annual report:

"As soon as possible after the end of each financial year, a responsible authority must prepare and send to the Department a report in respect of the carrying out of its functions under this Act during that financial year (an "annual report")."

"An annual report must include—

- (a) The authority's proceedings during the year;*
- (b) The authority's performance during that year;*
- (c) The number of security incidents and action's taken;*
- (d) Occasions premises that were entered under section 36(2)(d);*
- (e) Occasions premises that were entered under section 60(4)(d);*
- (f) any other information as the Department may direct."*

The reporting period is defined in Clause 20(10) as:

- "(a) the period of 2 years beginning with the day on which this section comes into force; and*
- (b) each successive period of 12 months."*

This ensures that the Department receives both an initial baseline report and annual updates thereafter.

Reporting by the Technical Authority

The Technical Authority also plays a key role in incident monitoring and reporting. Under Clause 20, one of its functions is:

"reporting to the Department on security incidents."

The content of the security report is comprehensive. Clause 20(3) specifies that it must include:

- Compliance with duties under sections 26, 27, 28, 29, 35(2)(a), 36 and 79.
- Extent of compliance with section 75 codes of practice.
- Information about security incidents reported under section 30.
- Actions taken by the authority in response to reported incidents.
- Extent and manner in which a responsible authority exercised functions under sections 34–43 and 81.
- Identification of risks to the security of national infrastructure.
- Any other information specified by the Department.

Additionally, Clause 32 empowers the Technical Authority to inform the Department when a security incident:

"could result in, or has resulted in—

- (a) a serious threat to the safety of the public, to public health or to national security; or*
- (b) the economic well-being of the Island; or*
- (c) serious economic or operational problems for entities."*

This ensures that the Department is kept informed of both actual and potential threats in real time, enabling swift policy or operational responses.

Section 11: Questions

Q29. Are the reporting obligations for Responsible Authorities and the Technical Authority in Clauses 13 and 20 clearly defined and appropriate?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Q30. Is the frequency and content of required reports for entities (e.g. annual reports, security reports) suitable for effective oversight?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Section 12: Implementation

The implementation of the National Infrastructure Security Bill marks a significant step forward in strengthening the resilience and security of the Isle of Man's national infrastructure. As organisations begin to engage with the new requirements, ranging from registration and classification to risk management, incident reporting, and compliance assessments, it is recognised that this transition may present operational and strategic challenges.

Organisations may need support in interpreting their obligations under the Bill, aligning existing practices with new standards, and developing the technical and organisational capabilities required to meet resilience and cybersecurity expectations. This could include assistance with risk assessments, incident response planning, supply chain security, and understanding the assurance frameworks and codes of practice that underpin compliance.

As the Cyber Security Centre for the Isle of Man, we are committed to making this transition as smooth and constructive as possible. Our role as the Technical Authority includes not only monitoring and advising on cybersecurity risks but also working collaboratively with entities to build capacity, share best practices, and provide clear, actionable guidance. We aim to be a trusted partner in helping organisations navigate the new regulatory landscape.

We welcome dialogue with all stakeholders and encourage organisations to reach out early for support. Whether you are seeking clarification on your classification, advice on technical measures, or assistance with reporting procedures, we are here to help. Together, we can ensure that the Island's infrastructure remains secure, resilient, and prepared for the challenges ahead.

Section 12: Questions

Q31. What support or guidance would your organisation need to comply with the proposed legislation?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?

Q32. What role should government play in helping smaller or less-resourced entities meet their obligations?

- ☐ Yes
- ☐ No
- ☐ Unsure

Any further comments?