NATIONAL INFRASTRUCTURE SECURITY BILL 202X

Index

NATIONAL INFRASTRUCTURE SECURITY BILL 202X

A BILL to provide for the security and protection of the national infrastructure; and for connected purposes.

BE IT ENACTED by the King's Most Excellent Majesty, by and with the advice and consent of the Council and Keys in Tynwald assembled, and by the authority of the same, as follows:—

PART 1 – OPENING PROVISIONS

1 Short title

The short title of this Act is the National Infrastructure Security Act 202x.

2 Commencement

(1) This Act commences on the day or days specified in an order made by the Department of Home Affairs.

(2) An order may specify that this Act commences on different days for different purposes.

PART 2 – FUNDAMENTAL PRINCIPLES

3 Infrastructure

(1) For the purposes of this Act —

(a) "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; and

(b) 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 or public health or safety.

(2) References to the —

(a) national infrastructure; and

(b) critical national infrastructure,

are to be construed as references to all, or any part, of that infrastructure.

(3) The critical national infrastructure consists of the sectors referred to in the tables in the Schedule.

(4) References to a "sector" include a sub-sector of that sector (see Schedule).

4 Security incident

(1) For the purposes of this Act, a **"security incident",** means —

(a) in relation to the national infrastructure generally, —

(i) anything that compromises the availability, performance or functionality of that infrastructure;

(ii) any unauthorised access to, interference with or exploitation of that infrastructure or anything that enables such access, interference or exploitation;

(b) in the case of a public electronic communications network or a public electronic communications service forming part of the national infrastructure, means (in addition to the matters referred to in paragraph (a)) the following —

(i) anything that compromises the confidentiality of signals conveyed by means of the network or service;

(ii) anything that causes signals conveyed by means of the network or service to be lost, unintentionally altered or altered otherwise than by or with the permission of the vendor of the network or service;

(iii) anything that occurs in connection with the network or service and compromises the confidentiality of any data stored by electronic means;

(iv) anything that occurs in connection with the network or service and causes any data stored by electronic means to be lost, unintentionally altered or altered otherwise than by or with the permission of the person holding the data;

(v) anything that occurs in connection with the network or service and causes a connected security incident.

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

(3) A security incident does not include anything that occurs as a result of conduct that—

(a) is required or authorised by or under any Manx enactment (whenever passed) which—

(i) makes provision which is in the interests of Island's national security;

(ii) has effect for the purpose of preventing or detecting crime or of preventing disorder; or

(iii) makes provision which is in the interests of the economic well-being of the Island so far as those interests are also relevant to the interests of its national security;

(b) is undertaken for the purpose of providing a person with assistance in giving effect to a warrant or authorisation that has been issued or given under such an enactment;

(c) is undertaken for the purpose of providing a person with assistance in exercising any power conferred by or under prison rules; or

(d) is undertaken for the purpose of providing assistance to a constable.

5 Registered providers and vendors

(1) For the purposes of this Act —

(a) a registered provider is a person who is registered in the register as an essential, important or unclassified provider;

(b) a vendor is a person who provides goods, services of facilities to a registered provider to be used by that provider in connection with the national infrastructure.

(2) The Schedule classifies, by reference to —

(a) the sector to which a person provides goods, services and facilities; and

(b) the number of workers engaged by that person in the provision of those goods, services or facilities,

whether that person must be registered as —

(i) an essential provider;

(ii) an important provider; or

(iii) unclassified provider.

(3) The Department may, by order, amend the Schedule.

PART 3 – THE AUTHORITIES

The responsible authorities

6 Responsible authorities

(1) For the purposes of this Act —

(a) the Isle of Man Financial Services Authority established under section 1 of the Financial Services Act 2008 is the responsible authority in respect of the financial services and banking sector of the national infrastructure referred to in the Schedule; and

(b) the Communications and Utilities Regulatory Authority (re-named under the Communications and Utilities Regulatory Authority Order 2020 (SD 2020/0550)) is the responsible authority in respect of all other sectors referred to in the Schedule.

(2) Nothing in this Act prevents the responsible authorities from acting jointly where they consider it appropriate or convenient to do so.

(3) Where this Act imposes a function on a responsible authority without specifying which of them is to exercise it, they may agree which of them is to do so.

(4) The responsible authorities must keep a record of any such agreement.

(5) The Department may, by order, amend subsection (1).

7 Overarching objective of responsible authorities

(1) The overarching objective of a responsible authority is to assure that the national infrastructure is well managed, resilient and secure and, to that end, an authority must oversee compliance with minimum acceptable levels of resilience and cyber-security in respect of that infrastructure established by, or under, this Act.

(2) Each authority must act in a way —

(a) that is compatible with the overarching objective;

(b) that it considers most appropriate for the purpose of furthering that objective.

8 Independence of responsible authority

Each responsible authority is independent of, and not subject to the control or direction of any of the following, —

(a) Tynwald;

(b) any Department;

(c) any statutory board;

(d) any Minister;

(e) any other person specified in regulations made by the Department.

Functions and powers of the responsible authorities

9 Functions and powers of responsible authority

(1) A responsible authority has the functions and powers provided by, or under, this Act.

(2) Without limiting subsection (1), an authority must —

(a) establish and maintain a register of persons who are required to be entered in it as registered providers;

(b) investigate security incidents;

(c) notify registered providers of the form and content of returns provided for under section 25;

(d) ensure that a registered provider complies with resilience and cyber security standards set out in regulations made by under section 12;

(e) otherwise ensure that those subject to the provisions of, or under, this Act comply with them;

(f) to ensure that registered providers comply with their security duties.

(3) An authority may 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.

10 The register

(1) The Department may, by regulations, make provision in respect of registration in the register.

(2) Regulations under subsection (1) must, in respect of the categories of person to be registered as a provider, provide for initial registration conditions.

(3) Initial registration conditions may include those concerning —

(a) the information a person must register;

(b) the manner and form of providing such information;

(c) the satisfaction of specified requirements which are a condition precedent to registration;

(d) the manner and form of proving satisfaction of such requirements;

(e) the publication of information in the register, including who is to publish and when publication need not take place.

(4) The regulations may make different provision for different categories of person, groups of persons or individuals who are required to be registered.

(5) The Department must ensure that initial registration conditions are proportionate to its assessment of the risk posed to the critical national infrastructure by the person in question.

(6) The Department must keep initial registration conditions under review.

11 General ongoing registration conditions

(1) Regulations under section 10 must make provision about conditions applicable to a provider once registered ("ongoing registration conditions").

(2) The Department may determine different ongoing registration conditions for different categories of registration or for different registered providers or groups of provider.

(3) Without limiting subsections (1) and (2), ongoing registration conditions may include those in respect of –

(a) the maintenance of accurate registration data and the carrying out of risk-based due diligence;

(b) the manner and form of notifying the Department of a change in a registered provider's registered details.

(c) authority to inspect registers or to provide information to law enforcement agencies.

(4) 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.

(5) The Department must keep ongoing registration conditions under review.

12 Regulations about resilience and cyber security standards

(1) The Department may, by regulations, make provision in respect of minimum standards in relation to —

(a) critical national infrastructure resilience; and

(b) cyber security.

(2) Without limiting subsection (1), the regulations may make provision about —

(a) the content of such standards;

(b) those who are to comply with the standards;

(c) the role of a responsible authority in respect of the standards;

(d) the role of the technical authority in respect of the standards;

(e) penalties for failure to comply;

(f) defences in respect of a failure to comply with the standards;

(g) the revision of such standards;

(h) the publication of such standards (including as revised);

(i) consultation;

(j) guidance about such standards.

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

13 Responsible Authority: annual report

(1) 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").

(2) An annual report must include—

(a) details the authority's proceedings during the year in question;

(b) details about the authority's performance during that year;

(c) details of the number of security incidents that the authority has been informed of during the reporting period and the action taken by it in response;

(d) a statement of the number of occasions during that year on which premises have been entered in pursuance of a duty imposed under section 36(2)(d);

(e) a statement of the number of occasions during that year on which premises have been entered in pursuance of a duty imposed under section 60(4)(d);

(f) any other information as the Department may direct.

(3) The Department must lay a copy of the report before Tynwald.

The Technical Authority

14 The technical authority

For the purposes of this Act, the technical authority shall be the Cyber Security Centre for the Isle of Man (part of Office of Cyber Security and Information Assurance) or its successor by whatever name known.

15 Independence of technical authority

In the exercise of its functions provided by or under this Act, the technical authority is independent, and not subject to the control or direction, of any of the following —

(a) Tynwald;

(b) any other part of the Office of Cyber Security and Information Assurance and the Department;

(c) any other Department;

(d) any statutory board;

(e) any Minister;

(f) any other person specified in regulations made by the Department.

16 Functions and powers of the technical authority

(1) The technical authority has the functions provided by, or under, this Act.

(2) Without limiting subsection (1) the technical authority has, in particular, the following functions —

(a) the provision of advice to the responsible authorities in respect of their functions and responsibilities under this Act;

(b) the provision of advice to a registered provider in respect of the providers functions and responsibilities under this Act;

(c) with the consent of the registered provider in question, technical monitoring of any goods, services or facilities provided by it to the national infrastructure for the purposes of identifying any risk, issue or anomalous activity in the interests of protecting the infrastructure;

(d) maintaining, monitoring and enhancing critical national infrastructure security including by "scanning", "domain name system blocking" and "sink-holing";

(e) considering and advising on critical national infrastructure matters outside the Island that may affect the Island;

(f) acting as, or establishing, a CSIRT;

(g) informing users of the critical national infrastructure of risks to it;

(h) reporting to the Department on security incidents;

(i) acting as a "single point of contact".

17 Scanning

(1) The technical authority may carry out proactive non-intrusive scanning of publicly accessible network and information systems in the Island, including those of registered essential and registered important providers.

(2) Scanning may only be carried out to —

(a) detect vulnerable or insecurely configured network and information systems; and

(b) to inform the registered provider's concerned of those matters.

(3) When carrying out the tasks referred to in subsection (1), the authority may prioritise particular tasks on a risk-based basis.

(4) The authority may, with the consent of the registered provider in question, conduct offensive assessments of a publicly accessible network and information system provided by that registered provider.

(5) "Offensive assessment" means a form of cyber-security evaluation in the form of a simulated attack on a network or system with a view to identifying any vulnerabilities in them.

18 Domain Name System blocking

(1) Where the technical authority determines that a domain name system abuse poses a risk to national security or to the security of a network and information systems in the Island, it may (in writing) require a domain name system service provider or domain registrar to take appropriate measures to neutralise the abuse.

(2) "Appropriate measures" must be taken within the period set by the Authority and must take account of the nature of the abuse.

(3) The types of abuse referred to in subsection (1) include —

(a) malware distribution;

(b) the use of a command and control model allowing one or more hackers to drive the actions of devices from a remote location (often referred to as "Botnet Attacks");

(c) the flooding of a server with internet traffic to prevent users from accessing connected online services and sites (often referred to as "Distributed Denial of Service Attacks");

(d) unauthorised changes to domain name system entries which result in users being redirected to a spoofed, malicious website rather than the legitimate site they were attempting to reach;

(f) unsolicited messages used to deliver other forms of domain name system abuse (for example, emails, text messages and internet postings) sent to a large number of recipients or posted in a large number of places (often referred to as "spam").

(4) In this section —

"**domain name system service provider**" means a registered provider providing —

(a) publicly available recursive domain name resolution services for internet end-users; or

(b) authoritative domain name resolution services for third-party use, with the exception of foundational servers in the domain name system hierarchy ("root name servers");

"**domain name system abuse**" is any activity that makes use of domain names or the domain name system protocol to carry out harmful or illegal activity;

"**domain name system**" means a hierarchical distributed naming system which enables the identification of internet services and resources, allowing

end-user devices to use internet routing and connectivity services to reach those services and resources.

19 CSIRT

(1) The CSIRT must, as far as is reasonably practicable —

(a) monitor and scan publicly accessible network and information systems to identify malicious activity, vulnerabilities and configuration errors; and

(b) take the action it considers necessary to resolve the vulnerabilities, configuration errors, or cyber threats arising from them.

(2) The CSIRT must take reasonable steps to understand current global cyber threats and how these may affect the Island, and take any action it considers necessary in response to those threats.

(3) The CSIRT must take reasonable steps to —

(a) raise awareness in the Island of cyber threats, the risks arising from them, responses and mitigations;

(b) enable and promote the sharing of cyber security information in the Island;

(c) enable, provide and co-ordinate the delivery of cyber security services;

(d) increase the level of cyber resilience in the Island to reduce the risk, and impact, of incidents.

(5) The CSIRT must represent the Island's cyber security interests within the Island and internationally, including by participating in international co-operation networks.

(6) The CSIRT may advise any person affected or potentially affected by a cyber-attack or the threat of one.

(7) In undertaking its function under paragraph (2), the CSIRT may —

(a) where it reasonably believes a person has information reasonably required to CSIRT to fulfil those functions, require that person to provide that information in such manner and at such times as CSIRT specifies in a written notice given to that person;

(b) analyse information received by it relating to incidents affecting the Island;

(c) take any action it considers necessary to mitigate, or assist in the mitigation of, the effect of those incidents; and

(d) advise any person affected or potentially affected by an incident.

20 Technical authority: security reports

(1) As soon as practicable after the end of each reporting period the technical authority must prepare and send to the Department a security report in respect of that period.

(2) A security report must contain such information and advice as the authority consider may best assist the Department in the formulation of policy in relation to the security of the national infrastructure.

(3) A security report must in particular include—

(a) information about the extent to which a registered provider has complied during the reporting period with the duties imposed on that person by or under sections 26, 27, 28, 29, 35(2)(a), 36 and 79;

(b) information about the extent to which a registered provider has acted during the reporting period in accordance with codes of practice issued under section 75;

(c) information about the security incidents that the authority have been informed of during the reporting period under section 30;

(d) information about the action taken by the authority during the reporting period in response to such incidents;

(e) information about the extent to which and manner in which a responsible authority has exercised the functions conferred on it by sections 34 to 43 and 81 during the reporting period;

(f) information about any particular risks to the security of the national infrastructure of which the authority has become aware during the reporting period;

(g) any other information of a kind specified in a direction given by the Department.

(4) Subsection (5) applies where the technical authority reasonably believes a person has information reasonably required to enable the authority to fulfil its functions in relation to a security report.

(5) The authority may, by written notice, require that person to provide that information in such manner and at such times as the notice specifies.

(6) A security report must not include personal data (within the meaning of article 4 of the Data Protection (Application of GDPR) Order 2018 (SD 2018/0143).

(7) The Department may —

(a) publish a security report it has been given pursuant to this section;

(b) disclose a security report to any person performing functions of a public nature for the purpose of enabling or assisting the performance of those functions.

(8) In publishing or disclosing a security report, the Department must have regard to the need to exclude from publication or disclosure, so far as is practicable, the matters which are confidential in accordance with subsection (9).

(9) A matter is confidential under this subsection if —

(a) it relates to the affairs of a particular person and its publication or disclosure would or might, in the authority's opinion, seriously and prejudicially affect the interests of that person; or

(b) in the authority's opinion, it affects or could affect the national security of the Island or the Island's economic wellbeing.

(10) In this section "reporting period" means—

(a) the period of 2 years beginning with the day on which this section commences; and

(b) each successive period of 12 months.

(11) References in this section to a security report include part of such a report.

21 Technical authority: single point of contact

(1) The technical authority is the single point of contact in respect of critical national infrastructure resilience and cyber-security standards.

(2) As the single point of contact the authority may —

(a) consult and cooperate with relevant law enforcement bodies;

(b) consult and cooperate with relevant regulatory bodies in the Island;

(c) co-operate with the responsible authorities to enable them to carry out their functions and fulfil their obligations under this Act;

(d) liaise with international bodies concerned with cyber security or infrastructure resilience (or both).

PART 4 –REGISTERED PROVIDERS: DUTIES

22 Registered provider classification

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.

23 Assurance framework regulations

(1) The Department must make regulations in respect of an assurance framework applicable to a registered essential or registered important provider.

(2) Different frameworks may be made in respect of the different sectors specified in the Schedule.

(3) Without limiting subsection (1), the regulations may make provision about —

(a) security and risk assessments and certifications;

(b) business continuity plans;

(c) the assessment of such plans;

(d) core service delivery roles in respect of registered providers;

(e) notification of changes in functions or goods, services or facilities provided by such a registered provider;

(f) the independent certification of a registered provider's compliance with the framework;

(g) on-site and off-site supervision of registered providers;

(h) the audit of registered providers;

(i) notifying the technical authority of security incidents;

(j) penalties for non-compliance which may be specified as a sum or as a percentage of a registered provider's turnover for a specified period or both;

(k) any other matters which the Department considers to ensure or enhance the security of the Island's critical national infrastructure.

(4) Before making regulations under this section, the Department must have due regard to any assurance framework for a registered provider suggested by the technical authority.

24 Registered unclassified providers

(1) A registered unclassified provider must comply with minimum resilience and cyber security standards specified in regulations under section 12.

(2) Each responsible authority may issue guidance about critical national infrastructure security and resilience measures in respect of the sectors of the national infrastructure for which it is responsible.

(3) A provider referred to in subsection (1) must have due regard to such guidance, but a failure by it to act in accordance with guidance does not of itself make that provider liable to legal proceedings before a court or tribunal.

25 Returns

(1) This section applies to a registered essential provider and a registered important provider.

(2) As soon as possible after the end of each financial year, a registered essential provider must give the responsible authority a return setting out how it has complied, and continues to comply, with the assurance framework set out in regulations made under section 23 and applicable to it.

(3) A return referred to in subsection (2) must —

(a) where paragraph (b) does not apply, be certified as true and accurate by a senior officer or member of the provider (or, where that provider is an individual, by that individual);

(b) in the case of a return submitted at the end of the third financial year following the year in which the person was registered under section 10 and every third year thereafter, be certified as true and accurate by an independent assessor whom the Department considers has the necessary experience and expertise to do so.

(4) An independent assessor is a person whom the Department considers has the necessary experience and expertise to carry out the certification referred to in subsection (3).

(5) The first annual return to be provided by an registered essential provider is to be provided at the end of the financial year in which that person was registered under section 10.

(6) As soon as possible after the end of the third financial year following the year in which a registered important provider was registered under section 10 and every third year thereafter, such a provider must give the responsible authority a return setting out how it has complied, and continues to comply, with the assurance framework set out in regulations made under section 23 and applicable to it.

(7) A return referred to in subsection (6) must be certified as true and accurate by a senior officer of the provider (or, where that provider is an individual, by that individual).

(8) A return under this section must—

(a) be in the form specified by the relevant responsible authority; and

(b) contain such information as that authority may specify.

(9) The responsible authority may, at the request of a provider, accept a return no later than 3 months after the end of the financial year in question.

(10) A provider contravenes this section if it —

(a) fails to provide a return in accordance with this section; or

(b) provides a return containing false or deliberately misleading information.

(11) Where a provider fails to provide a return under this section, the responsible authority may instruct a suitably qualified independent person to compile a return covering the matters referred to in subsection (2) or, as the case may be, subsection (5) and send it to the responsible authority.

(12) Costs associated with the return referred to in subsection (11) are to be borne by the provider in question.

26 Registered providers: duty to take risk-management measures

(1) A registered provider must take appropriate and proportionate technical, operational and organisational measures —

(a) to manage the risks posed to that part of the critical national infrastructure in which that provider operates or to which it supplies goods, services or facilities; and

(b) to prevent or minimise the impact of security incidents on recipients of their services.

(2) The measures referred to in subsection (1) must ensure a level of security appropriate to the risks posed, due regard being had to —

(a) the cost, and feasibility, of implementing such measures;

(b) the provider's exposure to the risk;

(c) the number of workers engaged by the provider;

(d) the likelihood of the occurrence of a security incident, its severity and its impact.

(3) The measures must include, at least, those concerning —

(a) risk analysis;

(b) incident handling;

(c) business continuity;

(d) supply chain security, including security-related aspects concerning the relationships between each provider and its direct suppliers;

(e) human resources security, access control policies and asset management.

(4) When considering which measures referred to in subsection 3(d) are appropriate, a provider must take into account the vulnerabilities specific to each direct supplier to it and the overall quality of the goods, services and facilities provided by each such supplier.

(5) Any risks identified in respect of supply chain security must be recorded by the provider in a risk register maintained by it.

27 Registered providers: duty to take security measures

(1) This section applies to a measure, or description of measures, specified in writing by the Department.

(2) A registered provider must take such measures, or description of measures, as are appropriate and proportionate for the purposes of—

(a) identifying an actual or threatened security incident;

(b) reducing the risks of such an incident; and

(c) preparing for the occurrence of such an incident.

(3) A measure, or description of measures, may be specified only if the Department considers that taking that measure or a measure of that description would be appropriate and proportionate for a purpose mentioned in subsection (2).

(4) A measure, or description of measures, may be specified to apply to –

(a) one or more providers;

(b) a group of providers;

(c) a category (or categories) of provider;

(d) a person registering as a provider.

PART 5 – SECURITY INCIDENTS

28 Registered providers: general duty to take measures in response to security incidents

(1) This section applies where a security incident occurs in relation to critical national infrastructure.

(2) A registered provider must take such measures as are appropriate and proportionate for the purpose of preventing adverse effects arising from that incident.

(3) If the incident has an adverse effect on the critical national infrastructure, a registered provider must take such measures as are appropriate and proportionate for the purpose of remedying or mitigating that effect.

29 Registered providers: further duty to take specified measures in response to security incident

(1) The Department, having consulted a responsible authority and considered the advice of the technical authority, may direct a registered provider to take specified measures in response to —

(a) a significant security incident;

(b) adverse effects of that incident on that infrastructure.

(2) A direction under paragraph (1) may specify—

(a) the adverse effects in question;

(b) the measure, or a description of measures, to be taken —

(i) in response to an incident, for the purpose of preventing adverse effects on the critical national infrastructure arising from that incident,

(ii) in response to an adverse effect, for the purpose of remedying or mitigating that adverse effect.

(3) A measure, or description of a measure, may only be specified under subsection (2)(b) if the Department considers that taking that measure or a measure of that description would be appropriate and proportionate for the purpose for which it is to be taken.

30 Registered providers: duty to notify technical authority of security incident

(1) A registered provider must, as soon as it may reasonably be done, notify the technical authority of—

(a) a potential or actual security incident that the provider considers may have or has had a significant impact on the critical national infrastructure in which it operates or the goods, services or facilities which it provides to the critical national infrastructure;

(b) any security incident that puts any person in a position to be able to bring about a further incident that would have a significant effect on the critical national infrastructure.

(2) A provider must, in any event, notify the authority no later than 24 hours after it becomes aware that the incident has occurred, or the potential threat arises.

(3) In determining for the purposes of this section 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 critical national infrastructure is, or would be, affected;

(b) the number of persons who use the infrastructure that are, or would be, affected by the effect on it;

(c) the size and location of the geographical area within which persons who use the infrastructure are or would be affected by the effect on its operation;

(d) the extent to which activities of persons who use the infrastructure are, or would be, affected by the effect on its operation.

(4) A notification must include, in addition to the provider's name and details of the goods, services or facilities to the critical national infrastructure, any of the following that is within that provider's knowledge at the time the notification is given —

(a) the time the incident occurred, or the potential threat arose;

(b) the current status of the incident or potential threat;

(c) the duration (actual or potential) of the incident;

(d) information concerning the nature and impact of the incident or potential threat;

(e) information concerning any, or any likely, impact of the incident or potential threat outside the Island;

(f) any other information that a registered provider considers may be helpful to the authority.

(5) The Department may by order amend subsection (2) to vary the time within which a notification must be given.

(6) The Department may by order amend this section to make further or alternative provision about the notification of incidents.

31 Registered providers: incidents - notifications and reports

(1) Where a registered provider has given the technical authority a notification referred to in section 30, it must give the authority —

(a) an interim report no later than 72 hours after the security incident occurred, or as the case may be, the potential threat arose;

(b) a final report no later than one month after the incident was dealt with, or as the case may be, the potential threat arose.

(2) The Department may make regulations in respect of interim and final reports.

(3) Without limiting subsection (2) the regulations may, in respect of reports, make provision about —

(a) their form;

(b) their content;

(c) the material (if any) to accompany them;

(d) time limits for their completion;

(e) the method of giving them.

(4) Nothing in this section prevents the authority from requiring any other report in respect of the incident or potential threat.

32 Technical authority informing the Department of security incident

(1) This section applies where the technical authority —

(a) becomes aware of a security incident; or

(b) considers that a security incident has occurred, or there is a risk of one occurring.

(2) The authority must inform the Department of the incident if the authority considers that it could result in, or has resulted, in any of the following—

(a) a serious threat to the safety of the public, to public health or to national security;

(b) a serious threat to the economic well-being of the Island;

(c) serious economic or operational problems for registered providers.

(3) The authority may inform the Department of the risk of or (as the case may be) the occurrence of the incident in a case where the duty in subsection (2) does not arise.

33 Technical authority informing others of security incident.

(1) This section applies where the technical authority —

(a) becomes aware of a security incident; or

(b) considers that a security incident has occurred or there is a risk of one occurring.

(2) The authority must take such steps as are reasonable and proportionate for the purpose of bringing the relevant information, expressed in clear and plain language, to the attention of any registered provider that may be adversely affected by the incident.

(3) The relevant information is—

(a) the existence of the risk of the incident occurring;

(b) the nature of the incident;

(c) the technical measures that it may be reasonably practicable for persons who use the critical national infrastructure to take for the purposes of—

(i) preventing the incident adversely affecting them;

(ii) remedying or mitigating the adverse effect that the incident has on them; and

(d) the name and contact details of a person from whom further information may be obtained about the incident.

(4) The authority may direct a registered provider to take steps specified in the direction for the purposes of informing persons who use or have used the national infrastructure of —

(a) the incident;

(b) the technical measures that may be taken by them for a purpose mentioned in subsection (3)(c).

(5) The authority may if it considers it to be in the public interest—

(a) inform the public of the incident;

(b) inform the public of the technical measures that may be taken by members of the public for a purpose mentioned in subsection (3)(c).

(6) It is the duty of the provider to comply with a direction given under this section within the period specified in the direction (which must be reasonable).

Securing compliance with security duties

34 General duty of a responsible authority to ensure compliance with security duties

A responsible authority must seek to ensure a registered provider complies with the duties imposed on it by or under sections 26 to 29 and 67 (a "security duty").

35 Power of responsible authority to assess compliance with security duties

(1) 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.

(2) Where an assessment under this section is carried out, a provider must—

(a) co-operate with the assessment; and

(b) pay the costs reasonably incurred by the authority in connection with the assessment.

36 Power of a responsible authority to give assessment notices

(1) This section applies for the purposes of an assessment under section 35 in respect of a registered provider.

(2) A responsible authority may by notice ("an assessment notice") impose on a registered provider a duty to do any of the following things—

(a) carry out specified tests or tests of a specified description in relation to the critical national infrastructure;

(b) make arrangements of a specified description for another person to carry out specified tests or tests of a specified description in relation to the critical national infrastructure;

(c) make available for interview a specified number of persons of a specified description who are involved in the provision of goods, services or facilities to the critical national infrastructure;

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

(e) permit an authorised person to observe any operation taking place on the premises that relates to the network or service;

(f) direct an authorised person to equipment or other material on the premises that is of a specified description;

(g) direct an authorised person to documents on the premises that are of a specified description;

(h) assist an authorised person to view information of a specified description that is capable of being viewed using equipment on the premises;

(i) comply with a request from an authorised person for a copy of the documents to which the person is directed and the information the person is assisted to view;

(j) permit an authorised person to inspect or examine the documents, information, equipment or material to which the person is directed or which the person is assisted to view;

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

(3) The references in subsection (2)(a) and (b) to tests in relation to the critical national infrastructure include references to—

(a) tests in relation to premises used in connection with the provision of goods, services or facilities to the critical national infrastructure;

(b) tests in relation to persons involved in the provision of goods, services or facilities to the critical national infrastructure.

(4) An assessment notice may impose on a provider a duty to carry out, or to make arrangements for another person to carry out, a test in relation to the goods or services that risk causing a security incident, loss to a person or damage to property only if the test consists of the use of techniques that might be expected to be used by a person seeking to cause a security incident.

(5) An assessment notice may not impose on a provider a duty to permit an authorised person to enter domestic premises.

(6) An assessment notice may not impose on a provider a duty to do anything that would result in the disclosure of documents or information in respect of which a claim to legal professional privilege could be maintained in legal proceedings.

(7) An assessment notice must, in relation to each duty imposed by the notice, specify the time or times at which, or period or periods within which, the duty must be complied with.

(8) An assessment notice must provide information about—

(a) the consequences of failing to comply with a duty imposed by the notice; and

(b) the right of appeal in respect of the notice to the Tribunal.

(9) An assessment notice may by further notice—

(a) be revoked by a responsible authority;

(b) be varied by a responsible authority so as to make it less onerous.

(10) In this section—

"**authorised person**" means an employee of, or person authorised by, a responsible authority ;

"**domestic premises**" means premises, or a part of premises, used as a dwelling;

"**specified**" means specified in the assessment notice.

37 Assessment notices: urgency statements

(1) This section applies where—

(a) an assessment notice is given under section 36 to a registered provider;

(b) the notice states that, in the responsible authority's opinion, it is necessary for the provider to comply with a duty imposed by the notice urgently;

(c) the notice gives the authority's reasons for reaching that opinion; and

(d) the notice provides information about the right of the provider to make an application under section 38.

(2) Subsections (8) and (9) of section 36 do not apply in relation to the duty mentioned in subsection (1)(b).

But see subsection (3) and (4) of this section.

(3) A time or period specified in an assessment notice under subsection (7) of section 36 in relation to the duty mentioned in subsection (1)(b) must not be one that falls or begins before the end of the period of 14 days beginning with the day the notice is given.

(4) In a case where—

(a) the duty mentioned in subsection (1)(b) is a duty to do something mentioned in section 36(2)(d) to (k); and

(b) the obligation to comply with the duty is appealed within 14 days beginning with the day the assessment notice under section 36 is given,

the provider need not comply with the duty in subsection (1)(b) pending the determination or withdrawal of the appeal.

38 Assessment notices: applications in respect of urgency statements

(1) This section applies where an assessment notice given under section 37 to a registered provider contains a statement under subsection (1)(b) of that section.

(2) The provider may apply to the Tribunal for either or both of the following—

(a) the disapplication of the statement in relation to some or all of the duties imposed by the notice;

(b) a change to the time at which, or period within which, a duty imposed by the notice must be complied with.

(3) On an application under this section, the Tribunal may do any of the following—

(a) direct that the notice is to have effect as if it did not contain the statement;

(b) direct that the inclusion of the statement is not to have effect in relation to a duty imposed by the notice;

(c) vary the notice by changing the time at which, or the period within which, a duty imposed by the notice must be complied with;

(d) vary the notice by making other changes required to give effect to a direction under paragraph (a) or (b) or in consequence of a variation under paragraph (c).

39 Enforcement of security duties

(1) Where a responsible authority determines that there are reasonable grounds for believing that a registered provider has failed to comply with a security duty it may give that provider a written notification under this section.

(2) A notification under this section is one which —

(a) sets out the determination made by the authority;

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

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

(d) specifies the steps that the authority think should be taken by the provider in question in order to—

(i) comply with the duty;

(ii) remedy the consequences of the contravention;

(e) specifies any penalty which the authority is minded to impose in accordance with section 40.

(3) A notification under this section—

(a) may be given in respect of more than one contravention of a duty; and

(b) if it is given in respect of a continuing contravention, may be given in respect of any period during which the contravention has continued.

(4) Where a notification under this section has been given, the authority may give a further notification in respect of the same contravention of that duty if, and only if—

(a) the contravention is one occurring after the time of the giving of the earlier notification;

(b) the contravention is a continuing contravention, and the subsequent notification is in respect of so much of a period as falls after a period to which the earlier notification relates; or

(c) the earlier notification has been withdrawn without a penalty having been imposed in respect of the notified contravention.

40 Penalties for contravention of security duties

(1) This section applies where a registered provider is given a notification under section 39 which specifies a proposed penalty.

(2) Where the notification relates to more than one contravention, a separate penalty may be specified in respect of each contravention.

(3) Where the notification relates to a continuing contravention, no more than one penalty may be specified in respect of the period of contravention specified in the notification.

(4) In relation to a continuing contravention, a penalty may be specified in respect of each day on which the contravention continues after the expiry of any period for complying with a requirement specified in the confirmation decision.

41 References to "enforcement" in sections 42 and 43

In section 42 and section 43—

(a) references to the commencement by the responsible authority of enforcement action in connection with a contravention are to the

giving of a notification under section 40 in respect of the contravention; and

(b) references to the completion by the responsible authority of enforcement action in connection with a contravention are to the taking of action in connection with the contravention.

42 Enforcement of security duties: proposal for interim steps

(1) This section applies where—

(a) a responsible authority determines that there are reasonable grounds for believing that a registered provider is contravening or has contravened a security duty;

(b) the authority either has not commenced, or has commenced but not completed, enforcement action in connection with the contravention;

(c) the authority determines that there are reasonable grounds for believing that either or both of the following conditions are met—

(i) a security incident has occurred as a result of the contravention;

(ii) there is an imminent risk of a security incident or (as the case may be) a further security incident occurring as a result of the contravention; and

(d) the authority determines that, having regard to the seriousness or likely seriousness of the incident or incidents mentioned in paragraph (c), it is reasonable to require the provider to take interim steps pending the completion by the authority of enforcement action in connection with the contravention.

(2) The authority may give a notification to the registered provider that—

(a) sets out the determinations mentioned in subsection (1);

(b) specifies the interim steps that the authority thinks the provider should be required to take pending the completion by the authority of enforcement action in connection with the contravention; and

(c) specifies the period during which the provider has an opportunity to make representations about the matters notified.

(3) In this section "interim steps" means—

(a) in a case where the authority determines that there are reasonable grounds for believing that a security incident has occurred as a result of the contravention, steps to—

(i) prevent adverse effects on the critical national infrastructure arising from the security incident;

(ii) remedy or mitigate any adverse effects on the critical national infrastructure arising from the incident;

(b) in a case where the authority determines that there are reasonable grounds for believing that there is an imminent risk of a security incident or (as the case may be) a further security incident occurring as a result of the contravention, steps to—

(i) eliminate or reduce the risk of the security incident or (as the case may be) the further incident occurring;

(ii) prevent adverse effects arising from the incident or (as the case may be) the further incident in the event it occurs.

43 Enforcement of security duties: direction to take interim steps

(1) This section applies where—

(a) a registered provider has been given a notification under section 42;

(b) the responsible authority has allowed the registered provider an opportunity to make representations about the matters notified; and

(c) the period allowed for the making of representations has expired.

(2) The authority may—

(a) direct the provider to take the interim steps or any of the interim steps specified in the notification; or

(b) inform the provider that a direction under paragraph (a) will not be given.

(3) The authority may give a direction under subsection (2)(a) only if (after considering any representations) it is satisfied—

(a) that there are reasonable grounds for believing that the contravention on the basis of which the notification was given occurred;

(b) that there are reasonable grounds for believing that either or both of the following conditions are met—

(i) a security incident has occurred as a result of the contravention;

(ii) there is an imminent risk of a security incident or (as the case may be) a further security incident occurring as a result of the contravention; and

(c) that, having regard to the seriousness or likely seriousness of the security incident or security incidents mentioned in paragraph (b), it is reasonable to give the direction.

(4) A direction under subsection (2)(a) must —

(a) include a statement of the authority 's reasons for giving the direction;

(b) in relation to each interim step, specify the period within which the step must be taken.

(5) A direction under subsection (2)(a) is ineffective in so far as it would require interim steps to be taken after the completion by the authority of enforcement action in connection with the contravention concerned.

(6) Where a direction under subsection (2)(a) has been given and has not been revoked, the authority must as soon as may reasonably be done—

(a) commence enforcement action in connection with the contravention concerned (unless enforcement action was commenced by authority before the direction was given); and

(b) complete enforcement action in connection with the contravention concerned.

(7) A direction under subsection (2)(a) may at any time—

(a) be revoked by the authority ; or

(b) be varied by the authority so as to make it less onerous.

(8) A provider given a direction under subsection (2)(a) must comply with it.

(9) That duty is enforceable in civil proceedings by the authority for an injunction, specific performance or any other appropriate remedy or relief.

44 Civil liability for breach of security duties

(1) A duty imposed by or under any of sections 26 to 29 and 67 on a registered provider is a duty owed to every person who may be affected by a contravention of the duty.

(2) Subsections (3) and (4) apply where a duty is owed by virtue of subsection (1) to a particular person.

(3) A breach of the duty that causes that person to sustain loss or damage is actionable at the suit or instance of that person.

(4) An act which—

(a) by inducing a breach of the duty or interfering with its performance, causes that person to sustain loss or damage; and

(b) is done wholly or partly for achieving that result,

is actionable at the suit or instance of that person.

(5) In proceedings brought against a provider by virtue of subsection (3), it is a defence for the provider to show that it took all reasonable steps and exercised all due diligence to avoid contravening the duty in question.

(6) The consent of the Attorney General is required for the bringing of proceedings by virtue of this section.

45 Statement of policy on ensuring compliance with security duties

(1) A responsible authority must prepare and publish a statement of its general policy with respect to the exercise of its functions under sections 35 to 44 and 81.

(2) An authority may from time to time revise that statement as it thinks fit.

(3) Where an authority makes or revises its statement of policy, it must publish that statement or (as the case may be) the revised statement in such manner as it considers appropriate for bringing it to the attention of the persons who, in its opinion, are likely to be affected by it.

(4) In exercising their functions under sections 35 to 44 and 81 an authority must have regard to the statement for the time being in force under this section.

PART 6 –DVNs AND DVDs

DVNs

46 DVNs

(1) The Department may issue a DVN designating a person ("the designated vendor") for the purposes of a DVD.

(2) A DVN may designate more than one designated vendor.

(3) The Department may issue a DVN only if it considers that the notice is necessary in the interests of national security.

(4) In considering whether to designate a vendor, the matters to which the Department may have regard include—

(a) the nature of the goods, services or facilities that are or might be supplied, provided or made available by the vendor;

(b) the quality, reliability and security of those goods, services or facilities or any component of them (including the quality, reliability and security of their development or production or of the manner in which they are supplied, provided or made available);

(c) the reliability of the supply of those goods, services or facilities;

(d) the quality and reliability of the provision of maintenance or support for those goods, services or facilities;

(e) the extent to which and the manner in which goods, services or facilities supplied, provided or made available by the vendor are or might be used in the Island;

(f) the extent to which and the manner in which goods, services or facilities supplied, provided or made available by the vendor are or might be used in other countries or territories;

(g) the registered provider of the persons concerned in—

(i) the development or production of goods, services or facilities supplied, provided or made available by the vendor or any component of them;

(ii) supplying or providing such goods or services or making such facilities available; or

(iii) providing maintenance or support for such goods, services or facilities;

(h) the registered provider of the persons who own or control, or are associated with—

(i) the vendor being considered for designation; or

(ii) any person described in paragraph (g);

(i) the country or territory in which the registered office or anything similar, or any place of business, of—

(i) the vendor being considered for designation; or

(ii) any of the persons described in paragraph (g) or (h),

is situated;

(j) the conduct of any of the persons described in paragraph (i) as it affects or might affect the national security of any country or territory;

(k) any other connection between a country or territory and any of those persons;

(l) the degree to which any of those persons might be susceptible to being influenced or required to act contrary to the interests of national security.

(5) A DVN must specify the reasons for the designation.

(6) The requirement in subsection (5) does not apply if or to the extent that the Department considers that specifying reasons in the notice would be contrary to the interests of national security.

(7) A reference in this section to a facility includes a reference to a facility, element or service that is an associated facility.

47 Further provision about DVNs

(1) Before issuing a DVN the Department must, so far as it is reasonably practicable to do so, consult the vendor or vendors proposed to be designated in it.

(2) The requirement in subsection (1) does not apply if or to the extent that the Department considers that consultation would be contrary to the interests of national security.

(3) Where a DVN is issued, the Department must send a copy to the person or person who are designated in it.

48 Variation and revocation of DVNs

(1) The Department must review a DVN from time to time.

(2) The Department may—

(a) vary a DVN;

(b) revoke a DVN (whether wholly or in part).

(3) The Department may vary a DVN only if it considers that the notice as varied is necessary in the interests of national security.

(4) Before varying a DVN, the Department must consult the person, or each of the persons, proposed to be designated in the notice as varied, so far as it is reasonably practicable to do so.

(5) The requirement in subsection (4) does not apply if or to the extent that the Department considers that consultation would be contrary to the interests of national security.

(6) The Department must, if or to the extent that it is reasonably practicable to do so, give notice of a variation to—

(a) any designated vendor under the DVN as the it had effect before the variation; and

(b) any vendor designated by the DVN as varied.

(7) The notice of variation must specify—

(a) how the DVN is varied;

(b) the reasons for the variation;

(c) the time at which the variation, or each of them, comes into force.

(8) The requirement in subsection (7)(b) does not apply if or to the extent that the Department considers that specifying reasons in the notice would be contrary to the interests of national security.

(9) The Department must give notice of a revocation to any designated vendor under the notice as it had effect before the revocation, if or to the extent that it is reasonably practicable to do so.

(10) The notice of revocation must specify—

(a) the time at which the revocation comes into force;

(b) if the DVN is partly revoked, what part of the notice is revoked.

49 DVN: laying before Tynwald

(1) The Department must lay before Tynwald a copy of—

(a) a DVN; and

(b) a notice of its variation or revocation.

(2) The requirement in subsection (1) does not apply if the Department considers that laying a copy of the notice before Tynwald would be contrary to the interests of national security.

(3) The Department may exclude from what is laid before Tynwald anything the publication of which the Department considers—

(a) would, or would be likely to, prejudice to an unreasonable degree the commercial interests of any person; or

(b) would be contrary to the interests of national security.

DVDs

50 DVDs

(1) The Department may give a direction under this section ("a DVD") to a registered provider.

(2) The Department may give a DVD 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 by it are proportionate to what is sought to be achieved by it.

(3) A DVD must specify—

(a) the registered provider or providers to whom the direction is given;

(b) the reasons for the direction;

(c) the time at which the direction comes into force;

(d) the vendor or vendors who are designated vendors under a DVN;

(e) a provider's right to appeal to the Tribunal against the direction or any requirement or condition of it.

(4) The requirement in subsection (3)(b) does not apply if or to the extent that the Department considers that specifying reasons in the direction would be contrary to the interests of national security.

(5) A DVD may impose requirements on a provider with respect to the use, in connection with the provision and operation of the critical national infrastructure, of goods, services or facilities supplied, provided or made available by the vendor or vendors specified in it and who are designated vendors under a DVN.

(6) A provider to whom a DVD is given must comply with it.

(7) A reference in this section to a facility includes a reference to a facility, element or service that is associated with that facility.

51 Further provision about requirements

(1) This section makes further provision about the requirements that may be imposed by a DVD.

(2) The requirements may include, among other things—

(a) requirements prohibiting or restricting the use of goods, services or facilities supplied, provided or made available by a registered provider specified in the direction;

(b) requirements prohibiting the installation of such goods or the taking up of such services or facilities;

(c) requirements about removing, disabling or modifying such goods or facilities;

(d) requirements about modifying such services;

(e) requirements about the manner in which such goods, services or facilities may be used.

(3) A requirement in a DVD may, among other things relate to the use of goods, services or facilities in —

(a) connection with a specified function of the critical national infrastructure provided by the registered provider;

(b) a specified part of the critical national infrastructure provided by the registered provider.

(4) A requirement in a DVD may make provision by reference to, among other matters—

(a) the source of goods, services or facilities that are supplied, provided or made available by a designated provider;

(b) the time at which goods, services or facilities were developed or produced (which may be a time before the passing of this Act);

(c) the time at which goods, services or facilities were procured by, or supplied, provided or made available to, the provider (which may be a time before the passing of this Act).

(5) A DVD may impose requirements that apply in specified circumstances (for example where a public communications registered provider is using goods, services or facilities supplied, provided or made available by one or more designated vendors).

(6) A DVD may provide for exceptions to a requirement.

(7) A requirement to do a thing must specify the period within which the thing is to be done.

(8) A period specified under subsection (7) must be such period as appears to the Department to be reasonable.

(9) In this section—

(a) a reference to a facility includes a reference to a facility, element or service that is associated with that facility;

(b) "specified" means specified in a DVD.

52 Consultation about DVDs

(1) Before giving a DVD, the Department must consult —

(a) the registered provider or providers to whom the proposed DVD may apply and the designated vendor or vendors who may be specified in it;

(b) the responsible authority; and

(c) any other person the Department considers appropriate.

(2) The requirement in subsection (1) does not apply if or to the extent that the Department considers that consultation would be contrary to the interests of national security.

53 Notice of DVDs

(1) Where a DVD is given the Department must, if or to the extent that it is reasonably practicable to do so, send a copy of the direction to the designated vendor or vendors specified in it.

(2) The requirement in subsection (1) does not apply, in the case of a designated vendor , if the Department considers that sending a copy of the direction to that designated vendor would be contrary to the interests of national security.

(3) The Department may exclude from the copy of the direction anything the disclosure of which the Department considers —

(a) would, or would be likely to, prejudice to an unreasonable degree the commercial interests of any person; or

(b) would be contrary to the interests of national security.

54 Variation and revocation of DVDs

(1) The Department must review a DVD from time to time.

(2) The Department may—

(a) vary a DVD;

(b) revoke a DVD (whether wholly or in part).

(3) The Department may vary a DVD only if it considers that —

(a) the direction as varied is necessary in the interests of national security; and

(b) the requirements imposed by the direction as varied are proportionate to what is sought to be achieved by the direction.

(4) Before varying a DVD the Department must, so far as it is reasonably practicable to do so, consult—

(a) the registered provider or providers who would be subject to the direction as proposed to be varied; and

(b) the person or persons who would be affected as a designated vendor or vendors by the direction as proposed to be varied.

(5) The requirement in subsection (4) does not apply if or to extent that the Department considers that consultation would be contrary to the interests of national security.

55 DVDS: notice of variation

(1) The Department must give notice of a variation of a DVD to the registered provider or providers subject to the direction as varied.

(2) The notice of variation must specify—

(a) how the direction is varied;

(b) the reasons for the variation;

(c) the time at which the variation, or each of them, comes into force.

(3) The requirement in subsection (2)(b) does not apply if or to the extent that the Department considers that specifying reasons in the notice would be contrary to the interests of national security.

(4) The Department must, if or to the extent that it is reasonably practicable to do so, send a copy of the notice of variation to the designated vendor or vendors specified in the direction as varied.

(5) The requirement in subsection (4) does not apply, in the case of a designated vendor , if the Department considers that sending a copy of the notice of variation to that designated vendor would be contrary to the interests of national security.

(6) The Department may exclude from the copy of the notice of variation anything the disclosure of which it considers—

(a) would, or would be likely to, prejudice to an unreasonable degree the commercial interests of the vendor or vendors subject to the direction as varied; or

(b) would be contrary to the interests of national security.

(7) The Department must give notice of a revocation of a DVD to the designated vendor or vendors referred to in the direction as it had effect before the revocation.

(8) The notice of revocation must specify—

(a) the time at which the revocation comes into force;

(b) if the direction is partly revoked, what part of the it is revoked.

(9) The Department must, if or to the extent that it is reasonably practicable to do so, send a copy of the notice of revocation to the designated vendor or vendors specified in the direction as it had effect before the revocation.

(10) The requirement in subsection (9) does not apply, in the case of a designated vendor, if the Department considers that sending a copy of the notice of revocation to that designated vendor would be contrary to the interests of national security.

(11) Where the direction is partly revoked, the Department may exclude from the copy of the notice of revocation anything the disclosure of which the Department considers—

(a) would, or would be likely to, prejudice to an unreasonable degree the commercial interests of any person; or

(b) would be contrary to the interests of national security.

56 DVDs: plans for compliance

(1) This section applies where a DVD has been given to a registered provider and has not been revoked.

(2) The Department may from time to time require the person to prepare a plan setting out the steps that the provider intends to take in order to comply with such requirements imposed by the direction as the Department may specify, and the timing of those steps.

(3) The Department may also require the person to give it and a responsible authority a copy of the plan.

(4) The Department may specify the period within which a plan is to be given to it or the authority.

(5) A period specified under subsection (4) must be one which appears to the Department to be reasonable.

57 DVDs: laying before Tynwald

(1) The Department must lay before Tynwald a copy of—

(a) a DVD; and

(b) a notice of its variation or revocation.

(2) The requirement in subsection (1) does not apply if the Department considers that laying a copy of the direction before Tynwald would be contrary to the interests of national security.

(3) The Department may exclude from what is laid before Tynwald anything the publication of which the Department considers—

(a) would, or would be likely to, prejudice to an unreasonable degree the commercial interests of any person; or

(b) would be contrary to the interests of national security.

Monitoring and enforcement

58 Monitoring of DVDs

(1) The Department may give a responsible authority a direction ("a monitoring direction") requiring that authority—

(a) to obtain information relating to a registered provider's compliance with a DVD;

(b) to prepare and send a report to the Department based on that information; and

(c) to provide it on request the information on which a report falling within paragraph (b) is based.

(2) The information that the authority may be required to obtain under subsection (1)(a) is—

(a) information that would assist the Department in determining whether the provider has complied, is complying or is preparing to comply with the DVD or a specified requirement imposed by it;

(b) information about a specified matter which is relevant to compliance with a requirement imposed by the DVD;

(c) if the provider has been required to provide a plan under section 56, information about whether the provider is acting in accordance with the plan.

(3) A monitoring direction may make provision about the form and content of a report.

(4) A monitoring direction may, in particular, require a report to include the authority 's analysis of information gathered by it and an explanation of that analysis.

(5) A monitoring direction may require the authority to give the Department separate reports on different matters.

(6) A monitoring direction may make provision about the time or times at which the authority must report to the Department, including provision requiring it to give reports at specified intervals.

(7) The authority must exercise its powers to obtain information in such manner as it considers appropriate for the purposes of preparing a report required by a monitoring direction.

(8) The Department may give an authority more than one monitoring direction in relation to a DVD.

(9) The Department may vary or revoke a monitoring direction.

(10) The Department must consult the authority before giving or varying a monitoring direction.

(11) In this section "specified" means specified in a monitoring direction.

(12) A responsible authority may, in writing, delegate the performance of its obligation under this section to the technical authority.

59 Reports made under monitoring directions

(1) The Department may—

(a) publish a report made by a responsible authority in accordance with a monitoring direction or part of it; or

(b) disclose such a report or part of it.

(2) In publishing or disclosing such a report, the Department must have regard to the need to exclude from publication or disclosure, so far as is practicable, the matters which are confidential in accordance with subsection (3).

(3) A matter is confidential under this subsection if—

(a) it relates to the affairs of a particular person and its publication or disclosure would or might, in the Department's opinion, seriously and prejudicially affect the interests of that person; or

(b) in the Department's opinion, its publication or disclosure would be detrimental to the Island's national security or economic wellbeing.

Inspection notices and enforcement directions

60 Power of the responsible authority to give inspection notices

(1) This section applies where the Department has given the responsible authority a monitoring direction under section 58 relating to a registered provider which has not been revoked.

(2) The authority may, by notice ("an inspection notice") given to the provider impose on that provider a duty to take any of the actions mentioned in subsection (4).

(3) The Authority may exercise the power in subsection (2) for the purpose of obtaining—

(a) information (in any form) that would assist the Department in determining whether the provider has complied or is complying with the DVD or a specified requirement of it;

(b) information (in any form) about a specified matter which is relevant to whether the provider has complied or is complying with a requirement imposed by the DVD.

(4) The actions are—

(a) to carry out surveys of a specified description of the goods, services of facilities provided by the provider;

(b) to make arrangements of a specified description for another person to carry out surveys of a specified description of those goods, services or facilities;

(c) to make available for interview a specified number of persons of a specified description who are involved in the provision of those goods, services or facilities (not exceeding the number who are willing to be interviewed);

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

(e) to permit an authorised person to observe any operation taking place on the premises that relates to the provision of the goods, services or facilities network, service or associated facilities;

(f) to direct an authorised person to equipment or other material on the premises that is of a specified description;

(g) to direct an authorised person to documents on the premises that are of a specified description;

(h) to assist an authorised person to view information of a specified description that is capable of being viewed using equipment on the premises;

(i) to comply with a request from an authorised person for a copy of the documents to which the person is directed and the information the person is assisted to view;

(j) to permit an authorised person to inspect or examine the documents, information, equipment or material to which the person is directed or which the person is assisted to view;

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

(5) An inspection notice may not impose on the provider a duty to permit an authorised person to enter domestic premises.

(6) An inspection notice may not impose on the provider a duty to do anything that would result in—

(a) the disclosure of documents or information in respect of which a claim to legal professional privilege; or

(b) a disclosure of documents or information that is prohibited by or under an enactment.

(7) An inspection notice must, in relation to each duty imposed by the notice, specify the time or times at which, or period or periods within which, the duty must be complied with.

(8) A time or period specified under subsection (7) must not be a time that falls or a period that begins before the end of the period of 28 days beginning with the day on which the inspection notice is given.

(9) In this section—

"**authorised person**" means an employee of, or person authorised by, a responsible authority ;

"**domestic premises**" means premises, or a part of premises, used as a dwelling;

"**specified**" means specified in an inspection notice.

61 Inspection notices: further provision

(1) An inspection notice must provide information about the consequences of failing to comply with a duty imposed by it.

(2) An inspection notice may by further notice—

(a) be revoked by the responsible authority;

(b) be varied by the authority so as to make it less onerous.

(3) Where an inspection notice is given to a registered provider, that provider —

(a) may not act in such a way as to defeat the purpose of the notice; and

(b) must pay the costs reasonably incurred by the authority in connection with obtaining information by means of the notice.

62 Notification of contravention

(1) The Department may give a person (P) a notification under this section where it determines that there are reasonable grounds for believing that P is contravening, or has contravened a requirement imposed by a DVD under section 50, or imposed under section 56, 67 or 72.

(2) A notification under this section is one which—

(a) sets out the Department's determination;

(b) specifies the requirement and contravention in respect of which the determination is made;

(c) specifies the period during which P has an opportunity to make representations;

(d) in the case or a requirement imposed by a DVD under section 50 or imposed under section 56, specifies the steps that the Department thinks should be taken by P in order to comply with the requirement and remedy the consequences of the contravention;

(e) in the case or a requirement imposed under section 67, specifies the steps that the Department thinks should be taken by P in order to bring the contravention to an end and remedy the consequences of the contravention;

(f) specifies the penalty which the Department is minded to impose.

(3) A notification under this section may be given in respect of more than one contravention.

(4) If a notification under this section relates to more than one contravention, a separate penalty may be specified under subsection (2)(f) in respect of each contravention.

(5) If a notification under this section is given in respect of a continuing contravention, it may be given in respect of any period during which the contravention has continued.

(6) If a notification under this section relates to a continuing contravention, no more than one penalty may be specified under subsection (2)(f) in respect of the period of contravention specified in the notification.

(7) Notwithstanding subsection (6), in relation to a continuing contravention, a penalty may be specified in respect of each day on which the contravention continues after—

(a) the giving of a confirmation decision under section 63 which requires immediate action in respect of that contravention; or

(b) the expiry of any period specified in the confirmation decision for complying with the requirement being contravened.

(8) Where a notification under this section has been given to P in respect of a contravention of a requirement, the Department may give a further notification in respect of the same contravention of that requirement if, and only if—

(a) the contravention is one occurring after the time of the giving of the earlier notification;

(b) the contravention is a continuing contravention, and the subsequent notification is in respect of so much of a period as falls after a period to which the earlier notification relates; or

(c) the earlier notification has been withdrawn without a penalty having been imposed in respect of the notified contravention.

63 Enforcement of notification

(1) This section applies where—

(a) a person ("P") has been given a notification under section 62;

(b) the Department has allowed P an opportunity to make representations about the matters notified; and

(c) the period allowed for the making of representations has expired.

(2) The Department may—

(a) give P a decision ("a confirmation decision") confirming the imposition of requirements on P in accordance with the notification under section 62; or

(b) inform P that no further action will be taken.

(3) The Department may not give P a confirmation decision unless, after considering any representations, it is satisfied that P has, in one or more of the ways specified in the notification under section 62, contravened a requirement imposed by a DVD under section 50 or imposed under section 56.

(4) A confirmation decision must be given to P without delay.

(5) A confirmation decision must include reasons for the decision.

(6) In the case of a requirement imposed in a DVD under section 50 or under section 56, a confirmation decision may—

(a) require immediate action by P to comply with the requirement specified in the notification under section 62, and to remedy the consequences of the contravention.

(7) In the case of a requirement imposed under section 67, a confirmation decision may

(a) require immediate action by P to bring to an end the contravention specified in the notification under section 62, and to limit the consequences of the contravention; or

(b) specify a period within which P must bring that contravention to an end and limit those consequences.

(8) A confirmation decision may also specify the steps to be taken by P in order to bring a contravention to an end or limit its consequences.

(9) A confirmation decision—

(a) may require P to pay the penalty specified in the notification under section 62 or such lesser penalty as the Department considers appropriate in the light of the matters referred to in subsection (8); and

(b) may specify the period within which the penalty is to be paid

(10) Those matters are —

(a) any representations made by P ; and

(b) any steps taken by P —

(i) in the case of a requirement imposed by a DVD under section 50 or imposed under section 56, to comply with the requirement specified in the notification under that section or to remedy the consequences of the contravention;

(ii) in the case of a requirement imposed under section 67, to bring the contravention to an end or to limit the consequences of it.

(11) P must comply with any requirement imposed by a confirmation decision.

(12) The Department may enforce P's duty in civil proceedings for an injunction, specific performance or any other appropriate remedy or relief.

64 Urgent enforcement direction

(1) The Department may give a direction under this section ("an urgent enforcement direction") to a registered provider if it determines that—

(a) there are reasonable grounds for believing that such a provider or vendor is contravening, or has contravened—

(i) a requirement imposed by a DVD under section 50; or

(ii) a requirement not to disclose imposed under section 67;

(b) there are reasonable grounds for suspecting that the case is an urgent case; and

(c) the urgency of the case makes it appropriate for the Department to take action under this section.

(2) A case is an urgent case for the purposes of this section if the contravention has resulted in, or creates an immediate risk of—

(a) a serious threat to national security; or

(b) significant harm to the security of the critical national infrastructure.

(3) An urgent enforcement direction must—

(a) specify the requirement and contravention in respect of which it is given;

(b) require the registered provider or designated vendor to take such steps falling within subsection (4) as are specified in the direction;

(c) specify a period within which those steps must be taken; and

(d) specify the Department's reasons for giving the direction.

(4) The steps falling within this subsection are the steps that the Department has determined are appropriate—

(a) for complying with the requirement; or

(b) for remedying the consequences of the contravention.

(5) The requirement in subsection (3)(d) does not apply if or to the extent that the Department considers that specifying reasons in the direction would be contrary to the interests of national security.

65 Urgent enforcement direction: confirmation

(1) As soon as reasonably practicable after giving an urgent enforcement direction, the Department must confirm or revoke the direction.

(2) The Department may confirm an urgent enforcement direction with or without modifications.

(3) The Department may confirm an urgent enforcement direction only if the Department has determined that—

(a) the registered provider or a designated vendor is contravening, or has contravened a requirement imposed by a DVD under section 50 or a requirement not to disclose imposed under section 67;

(b) the contravention has resulted in, or creates an immediate risk of a serious threat to national security or significant harm to the security of the critical national infrastructure; and

(c) it is appropriate to confirm the urgent enforcement direction, with any modifications, to prevent, reduce or remove that threat or harm or immediate risk.

(4) Before confirming an urgent enforcement direction, the Department must give notice to the registered provider or a designated vendor that it proposes to confirm the direction; and give them an opportunity of making representations about the grounds on which the enforcement notice was given and its effect and an opportunity of proposing steps to remedy the situation.

(5) The notice under subsection (4) must—

(a) state that the Department proposes to confirm the direction;

(b) specify any proposed modifications of the direction;

(c) specify its reasons for confirming the direction and for any modifications; and

(d) specify a reasonable period for making representations.

(6) The requirement in subsection (5)(c) does not apply if or to the extent that the Department considers that specifying reasons in the notice would be contrary to the interests of national security.

(7) As soon as reasonably practicable after determining whether to confirm the direction, the Department must by notice inform P of that fact.

66 Urgent enforcement direction: enforcement

(1) A registered provider given an urgent enforcement direction must comply with it, whether or not it has been confirmed (unless it is revoked).

(2) The duty is enforceable in civil proceedings by the Department for an injunction, specific performance or any other appropriate remedy or relief.

67 Requirement not to disclose

(1) 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.

(2) The Department may require a designated vendor not to disclose to any other person all or part of the contents of the DVN without its permission.

(3) The Department may require a person that has been given a notification under section 62 not to disclose to any other person the existence of the notification or all or part of its contents without its permission.

(4) The Department may require a person that has been given a confirmation decision under section 63 not to disclose to any other person the existence of the decision or all or part of its contents without its permission.

(5) The Department may require a person who has been given an urgent enforcement direction under section 64 not to disclose to any other person the existence of the direction or all of part of its contents without its permission.

(6) The Department may require a person who has been given a notice under section 65(4) or (7) not to disclose to any other person the existence of the notice or all or part of its contents without its permission.

(7) The Department may not impose a requirement on a person under subsections (1) to (6) unless the condition in subsection (8) is satisfied.

(8) The condition in this subsection is that the Department considers that it would be contrary to the interests of national security for—

(a) the contents of the DVD or the part specified under subsection (1);

(b) the contents of the DVN or the part specified under subsection (2);

(c) the existence or contents of the notification under section 62 or the part specified under subsection (3);

(d) the existence or contents of the confirmation decision under section 65 or the part specified under subsection (4);

(e) the existence or contents of the urgent enforcement direction or the part specified under subsection (5); or

(f) the existence or contents of the notice under section 65(4) or (7) or the part specified under subsection(6),

(as the case may be) to be disclosed, except as permitted by the Department.

(9) If the condition in subsection (10) is satisfied, the Department may require a person consulted under section 47(1), 48, 52, and 54 not to disclose to any other person—

(a) the existence of the consultation and any information disclosed to the person in the consultation; or

(b) the existence of a part of the consultation specified by the Department and any information disclosed to the person in that part of the consultation,

without it's permission.

(10) The condition in this subsection is that the Department considers that it would be contrary to the interests of national security for the matters described in subsection (9)(a) or (as the case may be) subsection (9)(b) to be disclosed, except as permitted by the Department.

(11) Where a person is subject to a requirement under this section not to disclose a matter, disclosure of that matter by an employee of the person or a person engaged in the person's business is to be regarded as a disclosure by the person, unless the person can show that the person took all reasonable steps to prevent such a disclosure.

(12) A requirement must be in writing.

Infrastructure Protection Orders

68 Infrastructure Protection Orders

(1) This section applies in respect of goods, services or facilities of an essential registered provider forming part of the critical national infrastructure.

(2) The Department may issue an infrastructure protection order where —

(a) it is satisfied there exists a serious threat to, or risk of significant impact on, those goods, services or facilities that confirms the existence, and magnitude, of that threat or risk; and

(b) it is satisfied that the threat or risk cannot be avoided or mitigated in any other way.

(3) An infrastructure protection order must be in writing and —

(a) identify the goods, services or facilities which the Department considers to be (or potentially be) at risk or subject to the threat;

(b) specify the registered essential provider or providers who are subject to the order;

(c) specify the measures that person or persons are required to take in order to prevent the risk or threat adversely affecting the goods, service or facilities in question or to remedy or mitigate the adverse effects of that risk or threat on them;

(d) be published in such a way as the Department considers will best bring it to the attention of those whom the Department considers would, or may, be affected by it.

(4) The publication of the order must be accompanied by an explanation, in clear and plain language, of its purpose and effect.

(5) An infrastructure protection order must be laid before Tynwald as soon as it may reasonably be done but is effective as soon as it is made.

(6) An infrastructure protection order is valid for a period of 3 months beginning with the date it is made and expires at the end of that period.

69 Monitoring of infrastructure protection orders

(1) The Department must —

(a) monitor compliance with an infrastructure protection order by a registered person who is subject to it;

(b) keep under review the need for the continuance of any order it has issued.

(2) For the purposes of subsection (1), an authorised person may —

(a) enter and inspect a registered person's premises;

(b) observe any operation taking place on the premises that relates to the goods, service or facilities supplied to, or forming part of, the national infrastructure;

(c) inspect equipment or other material on the premises connected to such goods, services or facilities or their supply;

(d) inspect documents on the premises that are connected to such goods, services or facilities or their supply.

(3) A registered person must not obstruct an authorised person in the execution of that person's functions referred to in subsection (2).

(4) For the purposes of this section —

"**authorised person**" means an employee of, or person authorised by, the Department ;

"premises" includes domestic premises.

70 Notifications to registered persons: Infrastructure protection orders

(1) Where the Department considers (whether following the actions of an authorised person or otherwise) that a registered person is not complying with an infrastructure protection order it may give that person a written notification under this section.

(2) A notification under this section is one which —

(a) sets out the determination made by the Department;

(b) specifies the non-compliance in respect of which that determination has been made;

(c) specifies the period during which the registered person in question has an opportunity to make representations;

(d) specifies the steps that the Department think should be taken by the registered person in question in order to comply with the infrastructure protection order and remedy the consequences of the non-compliance in question.

71 Rescission, variation and amendment

(1) The Department may rescind, vary or revoke an infrastructure protection order in accordance with this section.

(2) The Department may do any of the things referred to in subsection (1) of its own volition and at any time or upon the written application of any person who is the subject of the order in question.

(3) Before doing any of the things mentioned in subsection (1), the Department must carry out a further assessment of the threat or risk in respect of which the order was issued and of the likely effects of any action it may take under that subsection.

(4) An assessment referred to in subsection (3) must be documented in writing.

(5) The Department may rescind, vary or amend an order if satisfied that there are reasonable grounds for doing so having had regard to the current nature and severity of the threat or risk and any changes to those thing and the assessment referred to in subsection (3).

(6) The Department must publish in such a way as it considers will best bring it to the attention of those whom the Department considers would, or may, be affected by it any action it takes under this section and the effect of that action.

(7) The Department need not comply with subsection (6) if it considers that publication of all or any part of the order would be contrary to the interests of national security or the commercial interests of a person.]

PART 7 – INFORMATION PROVISIONS

72 Power of Department to require information etc

(1) The Department may require a person falling within subsection (2) 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.

(2) The persons falling within this subsection are—

(a) a person who is or has been an registered provider;

(b) a person not falling within paragraph (a) who appears to the Department to have information relevant to the exercise of its functions under sections 46 to 63 and 68 to 71.

(3) The Department may require a person falling within subsection (2)—

(a) to produce, generate or obtain information for the purpose of providing it under subsection (1);

(b) to collect or retain information that the person would not otherwise collect or retain for the purpose of providing it under subsection (1);

(c) to process, collate or analyse any information held by the person (including information the person has been required to collect or retain) for the purpose of producing or generating information to be provided under subsection (1).

(4) The information that may be required under subsection (1) includes, in particular, information about—

(a) the use, or proposed use, of goods, services or facilities supplied, provided or made available by a particular person or a particular description of person;

(b) goods, services or facilities proposed to be supplied, provided or made available by a particular person or a particular description of person;

(c) goods, services or facilities proposed to be supplied, provided or made available by a person who has not, or has not recently, supplied, provided or made available for use in the Island—

(i) goods, services or facilities of that description; or

(ii) any goods, services or facilities;

(d) the manner in which a public electronic communications network or a public electronic communications service is, or is proposed to be, provided or facilities that are associated facilities by reference to such a network or service are, or are proposed to be, made available;

(e) future developments of such a network or service or such associated facilities.

(5) The Department may require a person to provide information under this section at such times or in such circumstances as may be specified by it.

(6) A person must comply with a requirement imposed under this section in such manner and within such reasonable period as may be specified by the Department.

(7) The powers in this section are subject to the limitations in section 73.

(8) A reference in this section to a facility includes a reference to a facility, element or service that is associated with that facility.

73 Restrictions on imposing information requirements

(1) This section limits the purposes for which, and manner in which, requirements may be imposed under section 72.

(2) The Department is not to require a person to provide information under section 72 except by a notice served on the person that—

(a) describes the required information; and

(b) sets out the Department's reasons for requiring it.

(3) The Department is not to impose a requirement on a person under section 72(3) except by a notice served on the person that sets out the requirement and its reasons for imposing it.

(4) The requirements in subsections (2)(b) and (3) do not apply if or to the extent that the Department considers that setting out reasons in the notice would be contrary to the interests of national security.

(5) The Department is not to require the provision of information under section 72 except where the making of a demand for the information is proportionate to the use to which the information is to be put in the carrying out it functions.

(6) The Department is not to impose a requirement on a person under section 72(3) except where the imposition of the requirement is proportionate to the use to which the information required to be produced, generated, obtained, collected or retained (including information required to be produced or generated by processing, collating or analysing) is to be put in the carrying out of it functions.

(7) A requirement to provide information under section 72 does not require a person to disclose information in respect of which a claim to legal professional privilege could be maintained in legal proceedings.

74 Information sharing

(1) A person may disclose information to a relevant body for the purposes of the exercise of its functions and obligations under this Act.

(2) Information obtained by a relevant body in connection with the exercise of one of its functions may be used by it in connection with the exercise of any of its other functions.

(3) If both Condition A and Condition B are satisfied —

(a) a relevant body may share information with a body listed in subsection (6); and

(b) that subsection (6) body may share information with any other body listed in that subsection.

(4) Condition A is that the information sharing is necessary —

(a) for the purposes of the functions under this Act of the relevant body in question;

(b) in the interests of the security of the Island; or

(c) for purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution (whether inside or outside the Island).

(5) Condition B is that the information sharing is limited to information that —

(a) is relevant and proportionate to the purpose for which it is shared;

(b) is not confidential information; and

(c) is not information that may prejudice the security or commercial interests of a person.

(6) The bodies referred to in subsection (3) are —

(a) a relevant law enforcement authority;

(b) a public administration;

(c) any other person that a responsible authority, the technical authority or an registered provider considers appropriate.

(7) Information shared under subsection (4) or (5) may not be further shared by the person with whom it is shared under that paragraph for any purpose other than —

(a) a purpose mentioned in subsection (4) or (5); and

(b) with the consent of the relevant body in question.

(8) The Department may by order amend paragraph (6).

(9) "Relevant body" means, as the case may be, —

(a) a responsible authority;

(b) the technical authority;

(c) a registered provider.

75 Codes of practice about assurance frameworks

The Department may—

(a) issue a code of practice giving guidance as to assurance frameworks applicable to 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.

76 Issuing codes of practice about security measures

(1) Before issuing a code of practice under section 75 the Department—

(a) must publish a draft of the code or, where relevant, the revisions of the existing code;

(b) must consult the responsible authorities, registered providers to whom the draft would apply and such other persons as the Department considers appropriate about the draft; and

(c) may make such alterations to the draft as the Department considers appropriate following the consultation.

(2) Before issuing a code of practice under section 75 the Department must also lay a draft of the code before Tynwald.

(3) The Department must publish the code.

(4) A code of practice comes into force at the time of its publication under subsection (3), unless it specifies a different commencement time.

(5) A code of practice may specify different commencement times for different purposes and include transitional provisions and savings.

77 Withdrawing codes of practice about security measures

(1) Before withdrawing a code of practice under section 75 the Department must—

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

(b) consult the responsible authorities, registered providers to whom the code applies and such other persons as the Department considers appropriate, about it.

(2) Where the Department withdraws a code of practice, it must publish notice of the withdrawal of the code and lay a copy of the notice before Tynwald.

(3) A withdrawal of a code of practice has effect at the time of the publication of the notice of withdrawal under subsection (2), unless the notice specifies a different withdrawal time.

(4) A notice of withdrawal may specify different withdrawal times for different purposes and include savings.

78 Effects of codes of practice about assurance frameworks

(1) A failure by a person to act in accordance with a provision of a code of practice does not of itself make that person liable to legal proceedings before a court or tribunal.

(2) In any legal proceedings before a court or tribunal, the court or tribunal must take into account a provision of a code of practice in determining any question arising in the proceedings if—

(a) the question relates to a time when the provision was in force; and

(b) the provision appears to the court or tribunal to be relevant to the question.

(3) 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 if—

(a) the question relates to a time when the provision was in force; and

(b) the provision appears to the responsible authority to be relevant to the question.

(4) In this section—

(a) "code of practice" means a code of practice issued under section 75;

(b) "relevant function" means a function conferred on the responsible authority by sections 34 to 37, 42 or 43.

79 Duty to explain failure to act in accordance with code of practice

(1) This section applies where a responsible authority has reasonable grounds for suspecting that a registered provider is failing, or has failed, to act in accordance with a provision of a code of practice issued under section 75.

(2) The responsible authority may give the person a notification that—

(a) specifies the provision of the code of practice;

(b) specifies the respects in which the person is suspected to be failing, or to have failed, to act in accordance with it; and

(c) directs the person to give a responsible authority a statement under subsection (3) or (4).

(3) A statement under this subsection is one that confirms that the person is failing, or has failed, in the respects specified in the notification to act in accordance with the provision of the code of practice and explains the reasons for the failure.

(4) A statement under this subsection is one that states that the person is not failing, or has not failed, in the respects specified in the notification to act in accordance with the provision of the code of practice and explains the reasons for that statement.

(5) The person must comply with a direction given under subsection (2)(c) within such reasonable period as may be specified in the notification.

PART 8 – PENALTIES AND CLOSING PROVISIONS

80 Civil penalties

(1) If the responsible authority is satisfied that a person (P) —

(a) has contravened any provision of this Act;

(b) has contravened any prohibition or requirement imposed under this Act;

(c) in purported compliance with any such requirement, has made a statement which they know to be false, misleading or deceptive;

(d) in purported compliance with any such requirement, has furnished false, inaccurate or misleading information; or

(e) has falsified, concealed, destroyed or otherwise disposed of, or caused or permitted the falsification, concealment, destruction or disposal of documents which that person knows or suspects are or would be relevant to the discharge of any function, duty or investigation under this Act,

the authority may require the P to pay a penalty in respect of the matters referred to in this subsection.

(2) The authority must give written notice to P of any decision under subsection (1), together with a statement of the reasons for the decision.

(3) When setting the amount of a financial penalty, the authority must have regard to —

(a) the duration of the contravention, action or inaction of P;

(b) whether any steps have been taken to mitigate those things and the effect of such steps;

(c) the degree to which P has co-operated with the authority and any other person exercising functions under this Act;

(d) what is appropriate and proportionate to the contravention in respect of which it is imposed.

(4) 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.

(5) Where the notification under section 62 relates to a contravention of a requirement under section 51, 70 or section 71 —

(a) any penalty may not exceed £10 million; and

(b) any penalty specified under section 63(9), may not exceed £50,000 per day.

(6) This section applies where a sum is payable to the Department as a penalty under section 63.

(7) The penalty is recoverable as if it were payable under an order of a court.

(8) Where action is taken under this section for the recovery of a sum payable as a penalty under section 63, the penalty is to be treated for the as if it were a judgment entered in the court.

(9) In any other case, where P is —

(a) a registered essential provider, the maximum penalty is the greater of £2,000,000 and an amount equal to 2 per cent of P's total annual global turnover for P's most recent financial year;

(b) a registered important provider, the maximum penalty is the greater of £1,000,000 and an amount equal to 2 per cent of P's total annual global turnover for P's most recent financial year;

(c) a registered provider which is neither a registered essential provider nor a registered important provider, the maximum penalty is the greater of £500,000 and an amount equal to 1 per cent of P's total annual global turnover for P's most recent financial year

(10) An appeal against a decision under this section or the amount of a penalty (or both) lies to the Tribunal.

(11) A penalty is recoverable as if it were payable under an order of a court.

(12) Any amount received as a penalty shall be paid into and form part of the General Revenue.

(13) The Department may by order amend this section so as to substitute a different maximum penalty for the maximum penalty for the time being specified in subsection (4)(b) or (5).

(14) For the purposes of this section the turnover of P's relevant business for a period is to be calculated in accordance with such rules as may be set out in regulations made by the Department.

81 Offences and penalties

(1) A registered provider who contravenes section 22, 25, 26, 28, 29, 30, 31, 39, 68 or 70 is guilty of an offence and is liable —

(a) on summary conviction, to —

(i) a fine not exceeding five times level 5 on the standard scale;

(ii) a term of custody not exceeding 6 months; or

(iii) both;

(b) on conviction on information, to —

(i) a fine;

(ii) a term of custody not exceeding 2 years; or

(iii) both.

(2) Criminal proceedings in respect of any contravention of this Act may not be commenced or continued if the responsible authority has required a registered provider to pay a penalty under section 80 in respect of such contravention.

(3) No proceedings for an offence under this Act shall be commenced in the Island except by the Authority or by or with the consent of the Attorney General.

(4) Any document purporting to be the consent of the Attorney General for the commencement of proceedings for an offence under this Act and to be signed by the Attorney General shall be admissible as prima facie evidence without further proof.

82 Liability of "officers"

(1) Subsection (2) applies if —

(a) an offence referred to in section 80 is committed by a registered provider which is a body corporate, a partnership or an unincorporated body; and

(b) it is proved that an officer of that body or partnership authorised, permitted, participated in, or failed to take all reasonable steps to prevent, the commission of the offence.

(2) The officer, as well as the registered provider, is liable to the maximum penalty specified to in section 80(1).

(3) "Officer" includes —

(a) a director, secretary, partner, or other similar officer;

(b) a person purporting to act as a director, secretary, partner or other similar officer;

(c) if the affairs of the legal registered provider are managed by its members or council members, a member or council member;

(d) if the legal registered provider has a registered agent (within the meaning of the *Companies Act 2006*, the *Limited Liability Companies Act 1996* or the *Foundations Act 2011*), the registered agent.

(4) The Department may, by order, amend this section.

83 Defences

In respect of an offence referred to in section 80 or 81, it is a defence for a person referred to in those sections to prove —

(a) that the alleged offence was due to matters or circumstances beyond their control;

(b) that they took all reasonable precautions to prevent the commission of the offence;

(c) that they exercised all due diligence to prevent the commission of the offence;

(d) they acted with lawful authority.

84 Infrastructure Security Tribunal and appeals

(1) There shall be a tribunal known as the infrastructure Security Tribunal for the purposes of this Act and any other enactment in which an appeal lies to the Tribunal.

(2) The Tribunal shall consist of —

(a) a chairperson appointed in accordance with the Tribunals Act 2006; and

(b) 2 members selected in accordance with regulations made under section 9 of the Tribunals Act 2006, from a panel appointed in accordance with that Act.

(3) A registered provider and a designated vendor providing goods, services of facilities to such a provider aggrieved about any of the things referred to in subsection (2) may appeal to the Tribunal.

(4) Those things are —

(a) the issue of any direction, notice, order by or under this Act;

(b) any of the terms, requirements or conditions of a direction, notice or order referred to in paragraph (a);

(c) the imposition of a penalty under section 80 or 81;

(d) the amount of any such penalty.

(5) An appeal must be made in accordance with rules made under section 8 of the Tribunals Act 2006.

(6) On the determination of an appeal under this section the Tribunal shall —

(a) confirm, vary or revoke —

(i) the direction, notice or order in question;

(ii) the decision to impose a penalty;

(b) confirm, vary or remit the amount of the penalty.

(7) Any action taken by the tribunal shall not affect the previous operation of that direction, notice or order in question or anything duly done or suffered under it.

(8) Without limiting subsection (7), any decision of the Tribunal on an appeal under this section shall be binding on the body which issued the direction, notice or order or imposed the penalty and the applicant.

(9) An appeal shall lie to the High Court, in accordance with rules of court, on a question of law from any decision of the Tribunal.

85 Reviews

(1) The Department must, as soon as it may practicably be done after the end of the review period undertake a review of the operation and effectiveness of this Act and prepare and publish a report on the review.

(2) Without limiting subsection (1), the review must consider —

(a) whether the continuing operation of the Act is appropriate;

(b) the extent to which those with duties imposed by, or under, this Act have complied with them;

(c) the extent to which those with functions imposed by, or under, this Act have carried them out and how effective they have been in doing so;

(d) the adequacy of the assurance frameworks and resilience and cyber security standards established by, or under, this Act;

(e) the effectiveness of enforcement mechanisms provided for by, or under, this Act.

(3) When undertaking a review, to the extent the Department considers it necessary to fulfil the function referred to in subsection (1)(a), the Department (or, as the case may be, its delegate) must consult those with duties or functions imposed by, or under, this Act.

(4) The Department may delegate its functions under subsection (1) to any person it considers appropriate.

(5) The Department must, as soon as it may practicably be done after the report is prepared publish it and lay it before Tynwald.

(6) The "review period" means —

(a) a period of 5 years beginning with the day this Act is fully commenced;

(b) each subsequent period of 5 years.

86 Directions: formalities

(1) Directions must be in writing and laid before Tynwald.

(2) A direction is not a public document or a statutory document for the purposes of the Interpretation Act 2015 and the Legislation Act 2015.

87 Orders and regulations

(1) An order (other than one referred to in section 2) and regulations under this Act may include such consequential, incidental, supplementary, transitional and transitory provision as the maker of the instrument considers necessary or expedient.

(2) An order under section 2 is subject to section 34 of the Legislation Act 2015 (laying only).

(3) All other orders and all regulations under this Act subject to section 30 of the Legislation Act 2015 ("approval").

88 Interpretation

(1) In this Act —

"**connected security incident**" means—

(a) in relation to a public electronic communications network, a security incident that occurs in relation to another public electronic communications network or a public electronic communications service;

(b) in relation to a public electronic communications service, a security incident that occurs in relation to a public electronic communications network or another public electronic communications service;

"CSIRT" means a cyber security incident response team established by the technical authority (see Chapter 2) and referred to in section 20**;**

"cyber security" means the activities necessary to protect network and information systems, the users of those systems, and other persons affected by cyber threats;

"cyber threat" means any potential circumstance, event or action that could damage, disrupt or otherwise adversely affect network and information systems, the users of those systems and other persons;

"Department" means the Department of Home Affairs;

"designated person" means a person designated by a DVD;

"designated vendor " means a person designated by a DVN;";

"DVD" means a designated vendor direction referred to in section 50;

"DVN" means a designated vendor notice referred to in section 46;

"electronic communications service" means a service of any of the following types provided by means of an electronic communications network, except so far as it is a content service —

(a) an internet access service;

(b) a number-based interpersonal communications service; and

(c) any other service consisting of, or having as its principal feature, the conveyance of signals, such as a transmission service used for machine to machine services;

"financial year" means the period beginning with 1 April and ending on the following 31 March;

"Minister" means the Minister for the Department;

"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;

"network and information system" means —

(a) an electronic communications network;

(b) any device or group of interconnected or related devices, of which at least one performs automatic processing of digital data under a program; or

(c) digital data stored, processed, retrieved or transmitted by the network or device for the purposes of operation, use, protection and maintenance of the network or device;

"public electronic communications network" means an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to members of the public;

"public electronic communications service" means any electronic communications service that is provided so as to be available for use by members of the public;

"register" means the register established and maintained under section 10 and "**registered"** shall be construed accordingly;

"registered essential provider" means a person classified as an essential provider in the Schedule;

"registered important provider" means a person classified as an important provider in the Schedule;

"registered provider" is a person referred to in section 5;

"responsible authority" means the bodies referred to section 6;

"security duty" has the meaning given in section 34(1);

"urgent enforcement direction" has the meaning given by section 64.

(2) For the purposes of this Act, **"worker"** means an individual who—

(a) has entered into or works under a contract of service, apprenticeship or for services with the registered provider;

(b) is the holder of a public office, a director of corporate body or a person in employment with a public or local authority who, under a contract or arrangement, undertakes to do or perform personally any work or services for the registered provider; or

(c) under any other contract or arrangement, undertakes to do or perform personally any work or services for the registered provider.

(3) A contract or arrangement referred to in subsection (2)(b) and (c) may be —

(a) express or implied;

(b) oral or in writing.

(4) An "individual" referred to ins subsection (2) includes a volunteer.

SCHEDULE

NATIONAL INFRASTRUCTURE SECTORS

1 Introductory

The Tables in this Schedule —

(a) deal with, in each case, a specific sector of the national infrastructure;

(b) specify the elements and sub-sectors (if any) of each of those sectors;

(c) categorises a provider in an element, or subsector, of a sector as an —

(i) essential provider;

(ii) important provider; or

(iii) unclassified provider,

and does so by reference to the number of workers that person engages as a provider in respect of that element or subsector.

Table 1: Communications & Digital Services

Column 1 **Sector elements**	**Column 2** **Sub-sector**	**Column 3** **Categorisation of provider by number of workers engaged**		
		50 or more workers	**More than 25, but not more than 49, workers**	**More than 5, but less than 25, workers**
Communication services	Communications providers	Essential	Essential	Important
	Internet Service providers	Essential	Essential	Important
	Broadcasting Services	Essential	Important	Unclassified
	Satellite Communications	Essential	Essential	Important
	Supporting Infrastructure	Essential	Essential	Important
Digital Infrastructure services	Data Centres	Essential	Essential	Essential
	Cloud Service providers	Essential	Important	Unclassified

	Domain Name Systems	Essential	Essential	Essential
	Content Delivery Networks	Essential	Important	Unclassified
	Qualified Trust Services	Essential	Essential	Essential
	Trust Service providers	Essential	Important	Important
	Internet exchange point providers	Essential	Important	Unclassified
	TLD name registries	Essential	Essential	Essential
ICT Providers	Managed Services	Essential	Important	Unclassified
	Managed Security Services	Essential	Important	Unclassified
	IT Support Services	Essential	Important	Unclassified
Digital Providers	Online Marketplaces	Important	Important	Unclassified
	Search engines	Important	Important	Unclassified
	Social networking platforms	Important	Important	Unclassified
Domain Names	Domain Name Registration Services	Important	Important	Important

Table 2: Transport and Delivery Services

Column 1 **Sector elements**	**Column 2** **Sub-sector**	**Column 3** **Categorisation of provider by number of workers engaged**		
		50 or more workers	**More than 25, but not less than 50, workers**	**More than 5, but less than 25, workers**
Transport	Air transport	Essential	Important	N/A
	Rail transport	Essential	Important	N/A
	Road transport	Essential	Important	N/A
	Maritime transport	Essential	Important	N/A

	Logistics & freight	Essential	Important	N/A
Postal and Courier services	National postal services	Important	Unclassified	N/A
	Courier companies	Important	Unclassified	N/A
	Logistics vendors	Important	Unclassified	N/A
	Sorting and distribution centres	Important	Unclassified	N/A

Table 3: Energy

Column 1 Sector elements	**Column 2** Sub-sector	**Column 3** Categorisation of provider by number of workers engaged		
		50 or more workers	**More than 25, but not more than 50, workers**	**More than 5, but less than 25, workers**
Energy	Electricity	Essential	Important	Unclassified
	Oil & Gas	Essential	Important	Unclassified
	District heating	Essential	Important	Unclassified
	Hydrogen	Essential	Important	Unclassified
	Renewable energy	Essential	Important	Unclassified

Table 4: Health

Column 1 Sector elements	**Column 2** Sub-sector	**Column 3** Categorisation of provider by number of workers engaged		
		50 or more workers	**More than 25, but not more than 50, workers**	**More than 5, but less than 25, workers**
Health	Healthcare providers	Essential	Important	Unclassified
	Medical equipment manufacturers	Essential	Important	Unclassified
	Pharmaceutical companies	Essential	Important	Unclassified
	Public health	Essential	Important	Unclassified

	agencies			
	Research institutions	Essential	Important	Unclassified

Table 5: Water

Column 1 **Sector elements**	**Column 2** **Sub-sector**	**Column 3** **Categorisation of provider by number of workers engaged**		
		50 or more workers	**More than 25, but not more than 50, workers**	**More than 5, but less than 25, workers**
Water	Drinking water	Essential	Important	N/A
	Wastewater management	Essential	Important	N/A
	Water treatment plants	Essential	Important	N/A
	Reservoirs & storage	Essential	Important	N/A
	Distribution networks	Essential	Important	N/A

Table 6: Financial Services & Banking

Column 1 **Sector elements**	**Column 2** **Sub-sector**	**Column 3** **Categorisation of provider by number of workers engaged**		
		50 or more workers	**More than 25, but not more than 50, workers**	**More than 5, but less than 25, workers**
Banking	Commercial banks	Essential	Important	Unclassified
	Investment banks	Essential	Important	Unclassified
	Central banks	Essential	Important	Unclassified

Table 7: Public Administration

Column 1 **Sector elements**	**Column 2** **Sub-sector**	**Column 3** **Categorisation of provider by number of workers engaged**		
		50 or more workers	**More than 25, but not more than 50, workers**	**More than 5, but less than 25, workers**

Public Administration	Central Government Departments responsible for public administration (See Government Departments Act 1989)	Essential	Essential	Essential

Table 8: Space

Column 1 **Sector elements**	**Column 2** **Sub-sector**	**Column 3** **Categorisation of provider by number of workers engaged**		
		50 or more workers	**More than 25, but not more than 50, workers**	**More than 5, but less than 25, workers**
Space	Satellite operators	Essential	Important	Unclassified
	Ground stations	Essential	Important	Unclassified
	Launch services	Essential	Important	Unclassified
	Space-based services	Essential	Important	Unclassified
	Space manufacturing	Essential	Important	Unclassified

Table 9: Food & Manufacturing

Column 1 **Sector elements**	**Column 2** **Sub-sector**	**Column 3** **Categorisation of provider by number of workers engaged**		
		50 or more workers	**More than 25, but not more than 50, workers**	**More than 5, but less than 25, workers**
Food	Food processing	Important	Unclassified	N/A
	Food packaging	Important	Unclassified	N/A
	Food distribution	Important	Unclassified	N/A
	Wholesale	Important	Unclassified	N/A
Manufacturing	Industrial manufacturing	Important	Unclassified	N/A
	Consumer goods manufacturing	Important	Unclassified	N/A
	Pharmaceutical	Important	Unclassified	N/A

	manufacturing			
	Automotive manufacturing	Important	Unclassified	N/A

Table 10: Chemicals & Waste Management

Column 1 **Sector elements**	**Column 2** **Sub-sector**	**Column 3** **Categorisation of provider by number of workers engaged**		
		50 or more workers	**More than 25, but not more than 50, workers**	**More than 5, but less than 25, workers**
Chemicals	Chemical manufacturing	Important	Unclassified	N/A
	Petrochemicals	Important	Unclassified	N/A
	Pharmaceuticals	Important	Unclassified	N/A
	Agricultural chemicals	Important	Unclassified	N/A
	Chemical storage & distribution	Important	Important	Unclassified
Waste management	Waste collection	Important	Unclassified	N/A
	Waste treatment	Important	Unclassified	N/A
	Waste disposal	Important	Unclassified	N/A
	Recycling & recovery	Important	Unclassified	N/A

Table 11: Research

Column 1 **Sector elements**	**Column 2** **Sub-sector**	**Column 3** **Categorisation of provider by number of workers engaged**		
		50 or more workers	**More than 25, but not more than 50, workers**	**More than 5, but less than 25, workers**
Research	Research institutes	Important	Unclassified	N/A
	Collaborative research networks	Important	Unclassified	N/A

2 Interpretation

In this Schedule —

"Agricultural Chemicals" means fertilisers, pesticides, and other agrochemicals;

"Air Transport" means airports, airlines, air traffic control systems, and supporting infrastructure;

"Automotive Manufacturing" means the production of motor vehicles, parts, and related components;

Broadcasting Services" means radio and television broadcasting networks and services;

"Chemical Manufacturing" means the production of basic chemicals, specialty chemicals, and consumer chemicals;

" Chemical Storage and Distribution" means the storage and transportation of chemical products for industrial use;

"Cloud Services" means cloud computing services, including storage, processing, and software services (SaaS);

"Communications" means fixed and mobile telephony, broadband, and internet services;

"Consumer Goods Manufacturing" means the production of goods for consumer use, such as electronics, clothing, and household items;

"Content Delivery Networks (CDNs)" means networks of servers that deliver web content and services to users based on their geographic location;

"Courier Companies" means private companies providing expedited delivery services for documents and parcels;

" Distribution Networks" means pipelines and other infrastructure for transporting water to consumers;

"Data Centres" means facilities housing computer systems and associated components, such as telecommunications and storage systems;

" District Heating" means systems providing heating and cooling services to buildings and industries;

"Domain Name Systems (DNS)" means the internet's domain name system;

"Drinking Water Supply" means facilities and infrastructure for the extraction, treatment, and distribution of drinking water;

"Electricity" means power generation plants, transmission networks, and distribution systems;

"Food Distribution" means logistics and transportation services that deliver food products to retailers;

"Food Packaging" means the packaging and labelling of food products;

"Food Processing" means the processing of raw agricultural products into consumable food items;

"Ground Stations" means facilities that communicate with and control satellites;

"Healthcare Vendors" means hospitals, clinics, and other facilities offering medical services;

"Hydrogen" means the production, storage, and distribution infrastructure for hydrogen energy;

"Industrial Manufacturing" means the production of machinery, equipment, and industrial goods;

"Internet Services" means internet access and related services provided by internet service vendors;

"IT Support Services" means technical support and maintenance for ICT systems and infrastructure of Essential or Important Entities (i.e. supply chain);

"Launch Services" means launch services for satellites and other space assets;

" Logistics" means logistics and transportation services for mail and parcels;

"Logistics and Freight" refers to the transportation and logistics of goods;

"managed Security Services" means security management services, including monitoring, and managing security devices and systems;

"managed Services" means services related to the installation, management, operation, or maintenance of ICT products, networks, infrastructure, and applications;

"Maritime Transport" refers to ports, shipping companies, and maritime navigation systems;

"medical Equipment Manufacturers" means entities producing medical devices and equipment;

"National Postal Services means Government-operated postal services responsible for mail and parcel delivery;

"Oil and Gas" means extraction, refining, transportation, and storage facilities;

"Petrochemicals" means chemicals derived from petroleum and natural gas;

" Pharmaceuticals" means medicinal chemicals and pharmaceutical products;

"Pharmaceutical Companies" means entities involved in the production or wholesale distribution (or both) of medicines;

"Pharmaceutical Manufacturing" means the production of medical devices;

"Public Health Agencies" means governmental bodies responsible for public health and safety;

"Rail Transport" means railway operators, infrastructure managers, and supporting systems (but not heritage railways);

" Recycling and Recovery" means recycling materials and recovering energy from waste;

"Renewable Energy" means solar, wind, hydroelectric, and other renewable energy sources and their associated infrastructure;

"Research Institutes" means organisations dedicated to scientific, chemical and technological research but not medical and health-related research (for medical and health-related research see Table 4);

"Research Institutions" means entities conducting medical and health-related research;

"Reservoirs and Storage" means the infrastructure for storing water, including reservoirs and water towers;

"Road Transport" means road networks, traffic management systems, and public transportation services;

"Satellite Communications " means satellite-based communication services;

"Satellite Operators" means entities responsible for the operation and management of satellites;

"Sorting and Distribution Centres" means facilities where mail and parcels are sorted and distributed; "Space-Based Services" means services such as Earth observation and navigation;

"Space Manufacturing" means the production of spacecraft, satellites, and related components. "Supporting Infrastructure" means undersea cables, and other critical infrastructure supporting communication networks;

"Trust Services" means digital certificates and other trust services;

"Waste Collection" means the collection of industrial, and hazardous waste;

" Waste Disposal" means final disposal of waste in landfills or by incineration or through other facilities;

"Waste Treatment" means the treating waste to reduce its volume, toxicity, or environmental impact;

"Wastewater Management" refers to systems for the collection, treatment, and disposal of wastewater;

" Wholesale" means the wholesale distribution of food products.

"Water Treatment Plants" means facilities that treat water to meet safety and quality standards.