Economy

Consultation Response: Draft Cyber Security (Jersey) Law 202-

JULY 2024

Government of Jersey

Contents

Background

In order to establish the Jersey Cyber Security Centre as a technical advisory body that is independent from the Government of Jersey, legislation needs to be put in place outlining the scope of the work expected, an appropriate governance framework and the security requirements of those deemed to be Operators of Essential Services (OES).

During December 2023 and January 2024 an initial consultation was held to gather feedback on the proposed policy intent to draft a cyber defence law for Jersey. Specifically, feedback at this time was requested on the operational mandate of the Jersey Cyber Security Centre and obligations of entities to be captured as Operators of Essential Services. Feedback provided resulted in the draft of the Cyber Security (Jersey) Law 202- which was the basis of the second round of public consultation held in 2024.

During March and April 2024 the Government launched a public consultation to encourage feedback on the draft Cyber Security (Jersey) Law 202-. During this consultation period a broad range of Operators of Essential Services were engaged with to ensure feedback was received from a range of perspectives and views. Feedback was specifically requested on the following areas:

a) The definitions, scope and threshold requirements of Operators of Essential Services to be included;
b) The reporting obligations and time frame in which Operators of Essential Services are to report incidents to Jersey Cyber Security Centre;
c) Definition of 'significant incidents'; and
d) When the requirements on Operators of Essential Services should come into force.

Consultation engagement

The second consultation took place during March and April 2024. Feedback was collated at the sector-specific briefings, public meetings, through written feedback shared directly, and via response to the on-line survey form on the Government of Jersey cyber law consultation web page.

Over the course of the consultation period, 10 separate public briefings were held, reaching 93 participants, in addition to 27 private briefings, targeting potential Operators of Essential Services. This included security professionals, critical infrastructure providers, Jersey-based regulators, financial services, States owned entities, blue light services, government health and more. Publicity of the consultation period was supported via various newspaper articles, newsletter and social media advertising.

Feedback received at these meetings has been taken into consideration, alongside the 36 complete or partial responses captured via the online survey, and 14 email responses individually submitted via the economy@gov.je email address, representing a mix of individual and organisational responses.

A copy of the draft Cyber Security (Jersey) Law 202- and supporting consultation document were both publicly available via the gov.je consultation website throughout the consultation and remain publicly available.

Executive Summary

Overall, the feedback received during the consultation period, from both the written responses and from those attending the briefing sessions, was very supportive of the proposed cyber law for Jersey. Many participants recognised the importance of and the need for a cyber law to raise the cyber resilience of Jersey. The briefings were used to reiterate the policy intent that Jersey Cyber Security Centre (JCSC) is to be established as a technical advisory body and will not have any regulatory or enforcement powers.

Feedback during the consultation was specifically focused on Parts 4 and 5 of the draft Cyber Security (Jersey) Law 202- which relate to the definition of Operators of Essential Services and the threshold requirements for determining if an entity is captured as essential for Jersey and the duties placed on these entities.

Feedback was provided from all essential service sectors. This has resulted in refinement of some threshold requirements and a commitment to review the scope of Operators of Essential Services with a view to include further services in a second phase. For example, consultation will continue with Financial Services to refine the threshold for inclusion and further engagement will be sought with General Practitioners and Pharmacies.

The time frame for an Operator of Essential Service to provide notification of a cyber incident that has had or is likely to have a significant impact on the cyber security of the essential service provided will be 48 hours. Whilst there was support for 72 hours, to align with the Data Protection (Jersey) Law 2018 notification of a data beach requirement, as highlighted throughout the consultation, the notification requirements are different and require different information to be reported. The notification time period for reporting a significant cyber incident only starts after the incident has been identified and is classified by the organisation as 'significant'. It is ultimately intended that the notification to Jersey Cyber Security Centre forms an integral part of an operational incident response process, rather than being compliance led. On addressing these differences during the consultations, organisations understood that, in most cases, it would not be difficult to report very quickly after the incident had been assessed internally.

Some people expressed the view that Jersey is behind the times by not having a Jersey Cyber Security Centre. Noting the comparisons with the UK's 'technical authority' for cyber incidents, the National Cyber Security Centre being formed in 2016 and the Isle of Man launching the Office of Cyber Security and Information Assurance in 2017. Respondents recognised that the increasing level of geopolitical conflict and hybrid warfare, combined with the rise of organised cyber crime, meant that the risks to the Island were increasing and providing an effective regime for Jersey Cyber Security Centre was therefore urgent.

The below are examples of amendments to the Cyber Security (Jersey) Law 202- as a result of feedback:

1. Updated definitions in Part 1, to include revised 'cyber' definitions and refined definition of 'public administration';

2. Incident reporting timeframe to be a maximum of 48 hours after determining the incident is significant;
3. Refinement of the definition of Operator of Essential Service used in Article 24;
4. Removal of the financial services subsector from Operators of Essential Services, to work with industry on a suitable definition and threshold limits before being included;
5. Key Regulators explicitly included as Operators of Essential Services;
6. Removal of Article 32 which required the Operators of Essential Services to notify all impacted service users or network users of incidents;
7. Clarification of governance arrangements to ensure effectiveness and to be appropriate and proportionate to the size and scale of the Office of the Commissioner for Cyber Security;
8. Information sharing gateways have been clarified to ensure reporting to Jersey Cyber Security Centre does not contravene any other legal obligations an organisation may have.

During the latter part of 2024, guidance will be developed by Jersey Cyber Security Centre, with further consultation with each essential service sector, to support the legal duties placed on Operators of Essential Services. Due to the support received during the consultation, it has been proposed that the parts of the Cyber Law that impose duties on essential services will come into force up to 3 months after the initial enactment.

The planned review and update of the 2017 Cyber Security Strategy will also address some of the wider discussion points raised during the consultation period.

Summary of responses to consultation questions

Question 1: Do you consider the definition of Operators of Essential Services to be sufficiently broad to improve the baseline cyber resilience for Jersey?

Article 24 in the draft cyber law provided a definition of an Operator of Essential Service for Jersey. Feedback received supported this definition of Operators of Essential Services to improve the baseline for cyber resilience for Jersey, recognising that the cyber resilience of the jurisdiction extends beyond traditional critical infrastructure reflecting the reliance of network and information systems and digital connectivity in everyday life. This definition was highlighted at the public briefings and supported. Of the written responses, 66% agreed, 20% did not agree and 14% did not provide a response.

There is the policy intent to refine the definition of 'essential service' within Article 24 to reflect the language in Article 15 (3) (b), ensuring entities that would pose an *economic, reputational, political or wellbeing* risk to Jersey are clearly captured to help build the cyber resilience of the Island.

Feedback also suggested that the current definition could be extended in a phased manner over a number of years to capture further sectors and sub-sectors that, should they suffer a significant cyber incident, would pose an economic, reputational, political or wellbeing risk to Jersey. This is discussed further in responses to question 2. It should be noted that the Minister has the power to amend by Order the definition of a cyber threat or a cyber attack affecting Jersey, and therefore the Operators of Essential Services captured. This power by Order is to reflect the fast pace of technology development and its potential impact on Jersey.

Additional feedback provided in some cases was in relation to the threshold limits within Schedule 3, which for some sectors was seen as being too broad and captured entities beyond the original policy intent. This is discussed further in responses to question 9.

Question 2: Do you think there are any sectors or sub-sectors missing from the current definition of Operators of Essential Services? Please provide your rationale.

From the consultation discussions and written responses received the following sectors were considered to be missing from the definition of Operators of Essential services for Jersey. They were seen as either significant sectors for the economy, have a significant reputational impact on Jersey, or hold special category data and therefore pose a potentially high cyber risk:

- Hospitality services
- Construction industry
- Specific health care providers and pharmacy services, both private and government funded where their information technology provision is not supported by the Government Department Modernisation & Digital
- Service providers other than IT managed service providers within the supply chain of captured Operators of Essential services, on which the provisions of these services rely
- Air transport services and operations, including Air Traffic Control
- Coast Guard
- Professional Services notably accountants and law firms
- Jersey based regulatory bodies such as Jersey Financial Services Commission, Jersey Office of the Information Commissioner and Jersey Competition Regulatory Authority
- Payment Service Providers (PSPs) as a distinct separate sector
- Media services
- Inclusion of small to medium enterprises
- Jersey Heritage (the national archive)
- Jersey Development Company, Andium Homes and Jersey Overseas Aid, as companies owned or where States of Jersey is a majority shareholder

In the review of the feedback collated on missing categories and sub-categories the following comments are made and where relevant, amends will be made to the draft cyber security law:

- Updates will be made to the Transport Sector to ensure all *port* operations, air and sea, as defined within the Air and sea Ports (incorporation) (Jersey) Law 2015 are captured. It is not currently the policy intent to expand the definition to air transport carriers not based on Jersey. This decision will be revisited periodically to ensure the list of Operators of Essential services remains relevant for the jurisdiction.
- Updates will be made to the definition of 'public administration' to clearly define bodies in and out of scope and to be expanded to specifically include the three largest Jersey-based regulators that regulate between them a significant proportion of the defined Operators of Essential Services and themselves represent a key reputational risk for the Island. It is proposed that the following Jersey regulators to be captured under the amended definition are: Jersey Financial Services Commission, Jersey Office of the Information Commissioner and Jersey Competition Regulatory Authority.
- Updates will be made to the definition of 'public administration' will be made to capture Andium Homes and Jersey Development Company and Jersey Overseas Aid Commission. These entities have all been approached and are supportive of being included. Jersey Heritage will also be included in scope as they hold the national achieve on behalf of Jersey.

Health Community – currently only government services or digital health services supported by the Government department Modernisation & Digital are captured in scope. The policy intent is not to extend the current threshold limits at this stage, rather work with the health sector based on the consultation responses received. Due to the significant special category health data held by General Practitioners and Pharmacies, there is commitment to further engage with this sector to understand the scope of potential future amends to Operators of Essential Services for Jersey.

Observations were made that that the current threshold requirement for digital service providers will capture a number of small businesses. JCSC is committed to ensuring that the relevant guidance is developed and published before enactment of any duties that fall on Operators of Essential Services.

At this stage, it is not currently the policy intent to further expand the definition of Operators of Essential Services whilst the Jersey Cyber Security Centre is being established. Periodic reviews of the defined scope of essential services will be undertaken, in consultation with key stakeholders and Operators of Essential Services and the necessary amends will be made by the Minister via Regulations.

Question 3: Do you think there are any sectors or sub-sectors currently included in the definition of Operators of Essential Services that should be removed? Please provide your rationale.

Some responses received suggested that the definition of the following sectors were too broad and would capture more entities than the initial policy intent:

- Digital Sector – will be reviewed to further sub-divide the sector to provide additional clarity.
- Financial Services - the threshold levels for Banking and Financial Services are to be refined with key stakeholders. It is proposed that the legislation be lodged with a clearly defined threshold for Banking Services, and work will continue with Financial Services to develop an appropriate threshold definition, to be phased in via an amendment by Regulation.
- Public Administration Sector – as discussed in the response to question 2, will be reviewed to provide further clarity of the entities that are intended to be captured at this time.

Question 4: Do you agree with the mandatory reporting obligations placed on Operators of Essential Services?

Feedback received during the consultation period was supportive of the mandatory reporting obligations and that they appeared appropriate and proportionate. Of the written responses received 60% were in agreement, 24% were in disagreement and 16% did not provide a response. It was observed that a legal requirement to enable information to be shared with Jersey Cyber Security Centre would facilitate the sharing of relevant information, which was welcomed by perspective Operators of Essential Services. Jersey Cyber Security Centre is acutely aware that the information shared will be sensitive and has the relevant safeguards in place to manage this.

The current policy intent is to mandate that Operators of Essential Services must report a significant cyber incident to Jersey Cyber Security Centre within a stipulated timeframe. The initial notification will enable a dialogue between Jersey Cyber Security Centre and the Operators of Essential Service to be established. It has been observed in some jurisdictions, where incident reporting has been mandatory for a number of years, mandatory reporting requirements are moving to shorter initial reporting time frames and placing a requirement on their equivalent of Operators of Essential Services to submit updated information and a final report, both within specified time frames. This is not currently the policy intent and any future movement to this style of mandatory reporting regime would not be considered without consultation with Operators of Essential Services.

Feedback has also suggested reporting to Jersey Cyber Security Centre should align with various regulatory reporting requirements to Jersey-based regulators. However, the policy intent for the Cyber Law (Jersey) 202- is for the mandatory reporting of significant cyber incidents to Jersey Cyber Security Centre to eventually become an integral step within the organisations incident reporting process. This would initiate the sharing of information at an early stage, where knowledge of such information would have the greatest impact on improving the cyber resilience of the Island. The required information about the cyber incident does not need to be provided by legal and compliance teams and the law does not state that the notification must be in writing.

Depending on the nature of the incident, it is recognised that a requirement will be placed on Operators of Essential Services to report a significant cyber incident to Jersey Cyber Security Centre may overlap with existing regulatory requirements to report the incident with Jersey Competition Regulatory Authority, Jersey Finance Service Commission and the Data Protection Authority. In order to satisfy the requirements in the Draft Cyber Law, guidance will be developed, with input from essential services and published by Jersey Cyber Security Centre before enactment. The guidance will confirm what information is required and how the information can be submitted. It is the policy intent that the notification should not be an onerous task and the information to be able to be submitted for example, via telephone, email, in person or via the online form via the Jersey Cyber Security Centre website. For Jersey Cyber Security Centre, the quicker the information known at the time is shared, the more beneficial it is for Jersey. Notifications sent to Jersey Cyber Security Centre will not negate the need for the organisation to comply with any other legal or regulatory requirements. During the consultation it was voiced the desire to 'report once', for example via an online form, and for relevant bodies to draw down the required information for their needs. This interest has been fed back to the Department for the Economy for consideration in the future.

Question 5: The mandatory timeframes for an Operator of Essential Services to report a cyber incident being considered are 24, 48 or 72 hours. Please rate your preference with your first choice being your preferred and provide your rationale.

Preference for mandatory reporting times from written responses can be summarised as follows, taking % as a total of number of written responses for that timeframe. Not all responses provided a first, second and third choice:

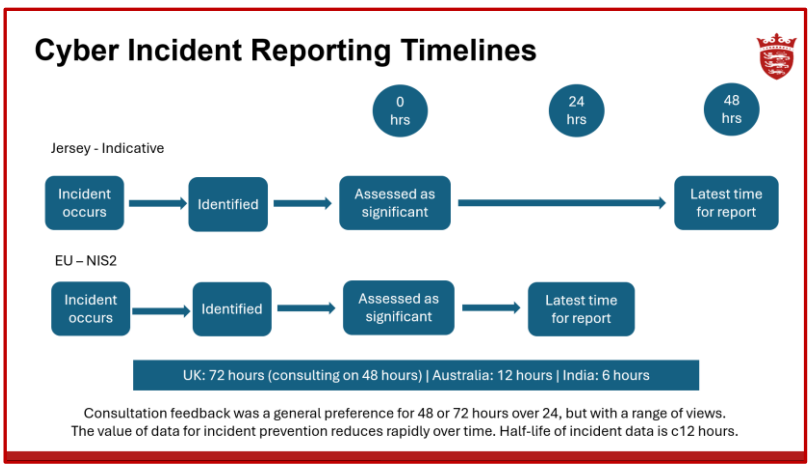
Response	Number of written responses:		
	24 hrs	**48 hrs**	**72hrs**
First Choice	14%	16%	50%
Second Choice	14%	50%	8%
Third Choice	44%	4%	24%
No preference stated	14%		

Within the Draft Cyber Law (Jersey) 202- Article 31 (1) places a duty on an OES to *notify the Commissioner of an incident that it considers to have had a significant impact on the continuity of the essential service which the OES provides.*

Drawing on the feedback received during the consultation, the policy intent is to clarify this duty to require Operators of Essential Services to notify the Commissioner of a *cyber incident that the OES considers has had, or is likely to have, a significant impact on the cyber resilience of the OES or on the essential service that the OES provides.*

Please see Appendix 1 for the revised definitions of 'cyber incident' and 'cyber resilience'. It is also the policy intent to expand the current definition 'essential service' to reflect the risks to Jersey as captured in Article 16 (3) (b), which are reputational and political as well as societal and economical.

In practical terms, the Operator of Essential Service first has to identify a cyber incident and secondly determine that the identified cyber incident can be categorised as a significant incident, as determined by Article 31 (2). This process is captured in the diagram below, which also compares the reporting times with the EU requirements:



Therefore, the reality is that the duty to report significant cyber incidents to the Commissioner within a given time period is only activated once the Operators of Essential Service has determined the cyber incident meets the relevant criteria to be classed as 'significant'. This process means there is already an inherent delay within the reporting timeframe. The sooner the information is shared with the Commissioner the more impactful the response from Jersey Cyber Security Centre. This was highlighted in some feedback supportive of a 48 hour reporting timeframe, for example:

> "early notification is essential to making the process effective, 48 hours should enable organisations reasonable time to assess and evaluate any disruption to services and to determine if indeed it was as a result of a Cyber related incident. We would request that the JCSC acknowledge that during the early stages of an incident it can be challenging for organisations to fully assess and evaluate the information ahead of this being reported, for instance if a third party is operating the essential service on our behalf as they would have to notify us first, then we would have to understand the situation."

> "Teams need time to respond but the quicker the notifications are, the better we will all be protected from threats."

> "We agree with your rationale for proposing 48 hours. Time is of the essence in analysing any cyber security incident. Although we are a small business without the depth of resource that a typical OES might enjoy, we would expect to act 24/7 in response to a report of a serious incident."

> "This aligns with reporting commitments defined by other organisations. The first 24 hours are usually very fluid with key investigations ongoing. Also incident reporting during weekends or Bank Holidays could be better managed if the 48 hour timeframe was restricted to business days."

> "An OES should endeavour to report a cyber incident to the Commissioner as soon as possible, preferably within hours of becoming aware, however, the focus during the first 24hrs of an incident is likely to be on containment, information gathering and establishing facts. therefore 48hrs seems to be the best option."

Feedback also acknowledged that a shorter reporting time of 12 hours was of benefit, as explained in this response:

> "24 hours aligns with EU reporting standards, even though the UK only has 72-hour reporting requirements (we feel that 72 hours is too long and should not be an option). Many other laws mention "without undue delay", and 24 hours should be achievable by all OES providers on the island. It is particularly important, as noted in the consultation document, that the first 24 hours are critical in any response to a cyber incident. If any incident has the potential to be more widespread, it will be beneficial for the JCSC to be aware of it so that they can notify other organisations across the island as quickly as possible. Also, if support is required to respond to the incident, this can be mobilised quicker – especially given that Jersey is a somewhat isolated community (in a global sense)."

Additionally, feedback was received from respondents requesting a 72 hour timeframe to allow reporting to be aligned to data protection breach notifications. Reporting a significant cyber incident to the Commissioner is not a regulatory requirement and does not need to be reported by legal and compliance teams prior to the notification being made. It is appreciated that some businesses may require any mandatory notification to have the relevant business approval to satisfy their own business requirements to meet a legal obligation. The Data Protection (Jersey) Law 2018, Article 20 requires all data breach to be reported in writing in a manner specified by the Authority. The proposed

Cyber Law does not require a particular means of notification. During the briefings, several people identified that it was likely that Jersey Cyber Security Centre would experience overreporting when the law becomes enforceable, similar to when the Data Protection (Jersey) Law 2018 came into force. To help mitigate this, JCSC are hosting several workshops for OES to help them understand with examples what is classified as a significant incident.

The policy intent is to have a maximum reporting time of 48 hours after a significant cyber incident has been identified. Relevant supporting guidance will to be developed and published to support this requirement. This duty does not prevent Operators of Essential Services, or indeed any other entity, voluntarily sharing incident information in an earlier timeframe or reporting cyber incidents not categorised as significant.

JCSC provided the following feedback during the consultation:

> "The information is most useful in the first 0-12 hours, then declines in value rapidly such that by 72 hours it is generally too late for JCSC to act to prevent contagion risk across the economy. We therefore support shorter timescales fully decoupled from regulatory obligations, as long as this does not lead to organisations prioritising reporting over remediation."

Question 6: Do you have any comments on the approach taken on the definition of significant incidents in Article 31 (2)?

Each essential service sector will have different requirements for determining whether a cyber incident is categorised as 'significant', taking into account the scale and impact of the incident as well as the scale and size of organisations. Therefore, Jersey Cyber Security Centre and Government have committed to hold sector-specific workshops during Q3 and Q4 2024 to develop guidance that will support essential service sectors to determine whether a cyber incident is significant. It is the policy intent that this guidance is developed and published before the legal obligations of Operator of Essential Services are enacted.

In one instance, clarity was sought on the use of 'it' within Article 31 (1). In this case 'it' refers to the Operator of Essential Service and it is the policy intent to review this drafting to ensure transparency.

In one response, a request was made to widen the definition to include 3rd party providers, where an Operator of Essential Service is made aware of an incident that could impact it or its clients. It is not currently the policy intent to widen the definition at this stage to 3rd party providers. Periodic reviews will be undertaken of essential sectors and sub-sectors and threshold limits to ensure they remain relevant for Jersey. This information about cyber incidents can also be shared with Jersey Cyber Security Centre on a voluntary basis and will be treated with the same level of confidentiality and respect as if reporting a significant incident.

Question 7: When do you think the all the requirements on Operators of Essential Services in Part 4 and /or Part 5 should come into force: immediately alongside the law; or at a later date?

	At a later date	Immediately alongside the law	Did not state
Number of written responses	58%	24%	18%

Feedback from the public briefings and 58% of written responses supported a delay in enactment for the requirements placed on Operators of Essential Services in Part 4 and Part 5. The majority of responses suggested a delay of between 3 to 12 months, with two respondents suggesting longer delays of 3 years and between 5 – 10 years.

It is the policy intent to delay the enactment of Parts 4 and 5 for up to 3 months, to enable the supporting guidance for Operators of Essential Services to be developed and published. Jersey Cyber Security Centre intend to develop this guidance with input from relevant essential service sectors prior to publication.

Article 40 determines that the Cyber Security (Jersey) Law 202- will come into force on a day to be specified by the Minister by Order, therefore dates of final enactments can be clearly communicated to all Operator of Essential Services in good time.

Question 8: Which Sector and/or Sub-Sector do you represent?

All Sectors and Sub-sectors identified as Operators of Essential Services within in the Draft Cyber Security (Jersey) Law 202-, were engaged with during the consultation period. They attended either public or private briefings where feedback was provided and, in some instances, this engagement was followed-up with written feedback.

Question 9: In your Sector/Sub-Sector, do you agree that the threshold limits as stated in the draft legislation would capture the key Operators of Essential Services for Jersey? Please provide your rationale.

Based on the feedback received during the consultation period the following threshold limits will be reviewed and amended:

Air and Sea Transport – it is the policy intent to capture the port operations licensed under Part 3 of the Air and Sea Ports (incorporation) Jersey Law 2015, where ports operations includes both harbour and airport services. These entities are headquartered in Jersey. The revised policy intent is not to capture international passenger operators at this stage, and threshold limits will be amended to capture this intent.

Banking and Financial Services Sector – policy intent is to revise these thresholds. The Banking subsector threshold will be refined and amended before lodging. The Financial Services subsector threshold will be removed for lodging to allow for further consultation on the threshold definition and re-introduced via amending Regulation in the future. Consultation will continue with this sub-sector to define relevant thresholds.

Digital Sector – additional sub-sectors will be included for ease of reference. These will include operators of the .je domain name; domain name services. Feedback highlighted that a number of smaller entities will be captured by the threshold limits.

Food retail – feedback was received to confirm whether the threshold of store size applied to a single store or groups of stores under the same Group. The threshold limit of '*a shop that has a retail sales area of 700 square meters or more*' applies to a single store, and wording of this threshold will be reviewed to ensure it reflects this.

Food distribution – based on feedback received, this threshold will be deleted. An unintended consequence of the threshold, as worded at the time of the consultation, captured very small local enterprises. Larger food retail spaces are captured via the thresholds in the food retail subsector, and food distribution falls under the currently worded road transport and freight distribution subsector.

Emergency Services – it is not the current policy intent to capture the coast guard, who are operated by Ports of Jersey Ltd. The threshold definition for air and sea transport will capture Ports of Jersey Ltd, and therefore by extension captures resources for co-ordinating maritime search and rescue within the Jersey Search and Rescue Region.

Government services – threshold limit will be refined for clarity. A new defined term "public administration" will capture Ministers, Parishes, Government Departments, an organisation listed in Schedule 2 of the Public Finances (Jersey) Law 2019, and Jersey Financial Services Commission, Data Protection Authority and Jersey Competition Regulatory Authority, due to their potential reputational risk should they have a significant cyber incident and Jersey Heritage trust due to their management archives held on behalf of Jersey.

Question 10: Do you have any other comments on Schedule 3?

The following comments were raised in response to this question. In some cases the question raised has been answered in the response to earlier questions.

- Airport Rescue and Fire Fighting Service – whilst it is based at Jersey Airport, it is maintained by Ports of Jersey. Ports of Jersey are captured as an Operator of Essential Service under the Transport Sector. Therefore, by extension the Airport Rescue and Fire Fighting Service will be included.
- Discharging reporting obligation to an IT service provider – further information will be provided in guidance. The legal duties lie with the designated Operators of Essential Services, how these are captured in contractual business arrangements with IT service providers is at the behest of the contracting parties.
- Application of the EU NIS and NIS2 definitions for Jersey – the policy intent has always been for best practice to be reviewed and adapted and adopted for Jersey, to enable improved cyber resilience for the jurisdiction. For European nations, NIS has been in force since 2018, and based on operational learnings. NIS2 expanded the sectors captured as essential for a jurisdiction and reduced reporting times for significant incidents to within 24 hours of becoming aware of and widened the definition of a 'significant' incident. These amendments have to be adopted by member states by October 2024. Likewise, there are other examples where nations are reviewing their current cyber security reporting requirements and sectors captured as critical entities for their jurisdiction to improve cyber resilience as reliance on technology increases. Australia updated its legislation in 2022, broadening its critical sectors and tightened mandatory cyber incident reporting obligations, requiring critical cyber incidents to be reported within 12 hours. In the United States, the Department of Homeland Security's Cyber Security and Infrastructure Security Agency is currently consulting on the scope of critical entities as well as the requirement to report a ransomware payment within 24 hours.
- Requirement for a dedicated, independent person with responsibility for Information Security – unlike the Data Protection (Jersey) Law 2018, there is not the requirement for Operators of Essential Services to put in place a dedicated trained and experienced resource with responsibility for Information Security. The initial policy intent for developing Jersey's cyber legislation was in response to the recommendation of the 2017 Cyber Security Strategy and supported by Ministers to establish a cyber resilience capability for Jersey. In order for Jersey Cyber Security Centre to prepare for, protect against and respond to cyber attacks on Jersey, cyber security information needs to flow into JCSC. Whilst it is acknowledged that a dedicated resource responsible for Information Security would enable this, requirement of Operator of Essential Services to implement such resource was out of the agreed policy scope. Operational learnings will be reviewed and this requirement may be part of future public consultations, as Jersey's cyber security resilience matures.

Additional feedback received

Article 32 – Duty to inform service users or networks users of incidents

Based on feedback received during the consultation period, Article 32 will be removed from the Cyber Security Law 202- in its entirety. The Data Protection (Jersey) Law 2018, Articles 20 (6) - (8), details provisions for requiring data subjects to be notified of data breaches. Beyond this notification, feedback received considered that any additional duty to notify service users or network users of cyber incidents, as currently drafted in Article 32, would see users receiving more notifications than were beneficial.

Definition of and threshold requirements of Operators of Essential Services

Periodic reviews will be made of the definition and threshold requirements of Operators of Essential Services to ensure they remain relevant as Jersey's digital and economic ecosystem matures and develops over time.

Technical Advisory Cells (TACs)

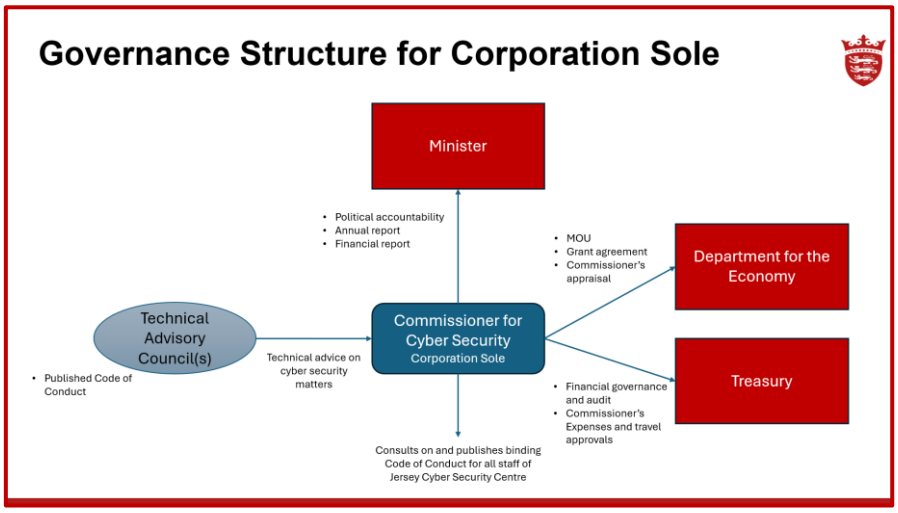
As detailed in Part 3, the objectives and functions of the Commissioner and the office of the Commissioner, JCSC, are to provide technical expertise, advice and support to raise the cyber resilience of the jurisdiction. Where expert advice and guidance is needed Technical Advisory Cells (TACs) will be established, drawing on international experts from both industry and academia. It may be that a TAC may see specific information is sought from Operators of Essential Services or that Operators of Essential Services may see to become members of a relevant TAC. A Code of Conduct will be developed and published before enactment. Terms of Reference will be developed before the first TAC is established and may be published.

Locally, two technical advisory groups have recently been established to grow the community of operators of essential services and cyber resilience for Jersey. The Cyber Suppliers Advisory Group and a Chief Information Security Officer (CISO) Group have been established in order to share information, best practice and provide advice to the Commissioner. Membership is by invitation and in due course all Operators of Essential Services will be invited to join a relevant group. Terms of Reference for both groups will soon be available on the JCSC website.

Governance of the Commissioner and Office of the Commissioner, the Jersey Cyber Security Centre (JCSC)

In the Draft Cyber Security (Jersey) Law 202- Article 4 (3) stated that the first Technical Advisory Cell would be established for the purpose of general oversight of the work of the Commissioner. During reviews of the legislation prior to lodging, this article is to be removed. Governance of the proposed corporation sole model will be through annual reporting (financial and deliverables) via the Minister. The necessary Memorandum of Understanding and Grant Agreement governance will be in place with the Department for the Economy, which will include relevant appraisal requirements of the Commissioner.

The Commissioner will be employed under contract and all Jersey Cyber Security Centre staff are considered States Employment Board Employees. Codes of Conduct will be developed and published on the JCSC website before the enactment of the legislation. The following diagram captures the governance structure of the Commissioner:



Article 14 - Fees

Article 14 enables the Commissioner for Cyber Security to charge back for a specific service provided. It is not the policy intent for the JCSC to be able to charge membership fees. The Commissioner will be grant funded through the Department for the Economy and there are no plans to change this funding mechanism.

Independence vs Involvement of the Minister

As a body corporate, the Minister has direct responsibility for the Commissioner. Article 8 (1) states that the Minister may only give guidance or directions to the Commissioner that will not compromise the independence of the Commissioner.

Information Sharing

Based on feedback and a review of Article 37, Information sharing by the Commissioner, the wording of this Article will be reviewed to ensure the policy intent is clearly articulated.

Appendix 1: Revised definitions

"cyber attack" means malicious or unauthorised activity that attempts to collect, disrupt, deny, degrade, destroy or reduce confidence in network and information systems or the information held in or processed through the systems;

"cyber incident" means an event –

(a) arising from a cyber threat;

(b) involving unauthorised access or attempted access to an organisation's network and information system, whether accidental or malicious;

(c) that compromises the confidentiality, integrity, availability, authenticity or non-repudiation of –

(i) network and information systems resources,

(ii) information held in or processed through the systems, #

(iii) the users of the systems, or

(iv) any other person; and

(d) that has a negative impact on the cyber security of those systems, information or persons.

"cyber resilience" means the capacity of a person to -

(a) to prepare for, protect against, detect, respond to or recover from a cyber threat in order to ensure the confidentiality, integrity, availability, authenticity or non-repudiation of network and information systems and information held in or processed through those systems; and

(b) to protect network and information systems, the users of those systems, and other persons from loss, disruption or harm;

"cyber risk" means a risk –

(a) associated with financial loss, disruption or damage to the reputation of an organisation; and

(b) arising from the failure of or unauthorised or erroneous use of its information and technology;

"cyber security" means the resilience of a person –

(a) to prepare for, protect against, detect, respond to or recover from a cyber threat in order to ensure the confidentiality, integrity, availability, authenticity or non-repudiation of network and information systems and information held in or processed through those systems; and

(b) to protect network and information systems, the users of those systems, and other persons from loss, disruption or harm;

"cyber threat" means an actual or potential circumstance or event –

(a) involving compromise of the confidentiality, integrity, availability, authenticity or non-repudiation of –

(i) network and information systems,

(ii) information held in or processed through those systems,

(iii) the users of those systems, and

(iv) other persons; and

(b) having the potential to negatively impact the cyber security of those systems, information or persons.

"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;