Economy

Consultation Draft Cyber Security (Jersey) Law 202-

5 MARCH 2024

Government of Jersey

Consultation Paper:

Contents

Consultation Paper: 2
Background 2
About the Consultation 3
Public Meeting dates 3
How to submit comments to the consultation 4
Data Protection 4
Draft Cyber Security (Jersey) Law 202- 5
PART 1 – Interpretations 5
PART 2 – Office of the Commissioner for Cyber Security 6
PART 3: Objectives and Functions of the Jersey Cyber Security Centre 7
PART 4: Operators of Essential Services 11
PART 5: Security Duties on Operators of Essential Services 12
Reporting a Cyber Security Incident to the Jersey Cyber Security Centre 12
Reporting a Cyber Security Incident to the users of a service 12
Enforcement provisions relating to Part 5. 13
PART 6: Administrative Provisions 16
Schedule 1 – Constitution of Jersey Cyber Security Centre 16
Schedule 2 Constitution of Technical Advisory Council 17
More than one Technical Advisory Council 17
Schedule 3 – Essential Services and Threshold Requirements 17

Background

As part of Jersey's efforts to be cyber resilient the Council of Ministers agreed the establishment of the Jersey Cyber Security Centre. This was a key recommendation in the 2017 Cyber Security Strategy. The creation of a cyber emergency response capability is integral to strengthening Jersey's national cyber resilience and international reputation. It is also vital for the continued growth and development of Jersey's economy.

Since June 2021, the Jersey Cyber Security Centre has operated within the Department for the Economy and has been funded as part of the Government Plan. The original name of the Cyber Emergency Response Team (CERT.JE) has been replaced by Jersey Cyber Security Centre (JCSC) to align with the reality that its remit is broader than just responding in the event of a cyber emergency.

The goal of Jersey Cyber Security Centre is to *prepare for, protect against, and respond to* cyber attacks on Jersey. Jersey Cyber Security Centre should be able to engage and communicate with industry, public bodies and the third sector as well as develop clear standards, expectations and support for cyber security risk management, control and assurance (*protect against*) and have the ability to monitor threats to the island and respond to major incidents (*respond to*). These capabilities will provide the Island with a balanced approach which enables the cyber risk profile of the Island to be reduced over time, whilst providing a proactive service to reduce the significant cyber security risks Jersey faces.

It is the intention for the Jersey Cyber Security Centre to become an independent advisory and emergency response body. This will allow Jersey Cyber Security Centre to operate at arm's length from regulators, law enforcement officers and government as a grant funded body. In order to establish the Jersey Cyber Security Centre as an arm's length corporation sole, legislation needs to be put in place outlining the scope of the work expected of the Jersey Cyber Security Centre and the associated governance.

It is the policy intent that the services and functions provided by the Jersey Cyber Security Centre are aligned with globally recognised services and functions provided by other national cyber emergency centres. The Jersey Cyber Security Centre is actively pursuing membership of the Forum of Incident Response and Security Team (FIRST.org), a global network of cyber security centres and specialists. In addition, the Jersey Cyber Security Centre has already become an accredited member of the Task Force Computer Security Incident Response Team (TF-CSIRT) community.

About the Consultation

The purpose of this consultation is to encourage feedback on the draft Cyber Security (Jersey) Law 202-, in particular the threshold requirements for Operators of Essential Services. In order to establish the Jersey Cyber Security Centre as independent from the Government of Jersey, legislation needs to be put in place outlining the scope of the work expected, appropriate governance and the security requirements of those deemed to be Operators of Essential Services (OES).

Public Meeting dates

During the consultation period specific briefings will be given as follows:

- Wednesday 6 March 2024 - Briefing for Critical National Infrastructure (CNIs) on the proposed new law at the CERT.JE office from 12pm to 1:30pm.
- Thursday 7 March 2024 briefing for general public from 17:00 – 18:30.
- Friday 8 March 2024 Briefing for Operators of Essential Services on the proposed new law at the Jersey Cyber Security Centre office from 08:00 – 09:00.
- Friday 8 March 2024 briefing for general public from 12:00 – 13:30.

All briefings will be held at the JCSC office. Additional briefings as per demand for targeted sectors.

How to submit comments to the consultation

Questions

The consultation is structured around a series of questions on Operators of Essential Services, which refer to specific sections of the Law. In your response, you should answer the questions in reference to the sections outlined.

You can submit your response to be received before 10:00 on Tuesday 23 April 2024:

- On-line via completing the online survey found at ***Cyber Law Consultation*** webpage
- By email to economy@gov.je with the subject heading ***Cyber Law Consultation***
- By post to: FAO Elisabeth Blampied, Department for the Economy, 19-21 Broad Street, St Helier, JE2 3RR

Data Protection

The information you provide will be processed in compliance with the Data Protection (Jersey) Law 2018. For more information, read the Department for the Economy Privacy Notice

The Government of Jersey may quote or publish responses to this consultation, but will not publish the name and addresses of individuals without consent. Types of publishing may include, for example, sending to other interested parties on request, sending to the Scrutiny Office, quoting in a published report, reporting in the media, publishing on the Government website, and listing on a consultation summary. Confidential responses will still be included in any summary of statistical information received and views expressed. We request that you do not provide any personal data within the free text boxes.

Under the Freedom of Information (Jersey) Law 2011, information submitted to this consultation may be released if a Freedom of Information request requires it, but no personal data may be released.

Draft Cyber Security (Jersey) Law 202-

There are 7 parts to the draft Cyber Security (Jersey) Law 202-. Each part is listed below Parts 4 and 5 and Schedule 3 have specific questions we would like you to consider when responding to this consultation.

PART 1 – Interpretations

This contains the key definitions of words and phrases used within the draft law. Definitions already defined in the Schedule Part 1 to the Interpretation (Jersey) Law 1954. "Island" shall mean the Island of Jersey and its dependencies and "Jersey" shall mean the Island of Jersey and its dependencies.

The Jersey Cyber Security Centre has a defined operational mandate for Jersey. The Jersey constituency definition can be found in the Jersey Cyber Security Centres RFC 2350. An RFC2350 is a document that specifies the general Internet community's expectations of Computer Security Incident Response Teams (CSIRTs). The Jersey Cyber Security Centre's RFC 2350 is publicly available on their website - https://cert.je/rfc2350.pdf.

The constituency of the Jersey Cyber Security Centre is the jurisdiction of Jersey, including:

a. all organisations established within the jurisdiction, including but not limited to the States of Jersey, public sector organisations, private and public companies, charities and third sector organisations

b. critical national infrastructure providers operating services in Jersey (regardless of domicile)

c. individuals resident in Jersey

d. the .JE top level domain name (gTLD), and

e. services using telephone and IP ranges allocated to Jersey telecoms providers or for use in Jersey.

Effectively this reflects where cyber incidents would lead to reputational, political, economic or wellbeing risks to the jurisdiction or its residents.

PART 2 – Office of the Commissioner for Cyber Security

This provides for:

1. The Office of the Commissioner for Cyber Security to be independent of the Government of Jersey, the Minister of Sustainable Economic Development and the States.
2. The establishment of the Jersey Cyber Security Centre.
3. The established of one or more Technical Advisory Councils. It is the policy intent for these individuals to provide advice and guidance to the Commissioner for Cyber Security and the Minister. The first Technical Advisory Council will provide general oversight of the work of the Commissioner for Cyber Security of the Jersey.
4. Codes of Conduct for both the Jersey Cyber Security Centre and the Technical Advisory Councils.
5. Governance requirements including Jersey Cyber Security to provide annual reports, audited accounts and a strategic plan.
6. The ability for Jersey Cyber Security Centre to charge fees in limited circumstances. For example if the Jersey Cyber Security Centre brings over a trainer to train several suppliers they would may charge the suppliers to attend to recover the cost to the taxpayer. Another example would be the ability to attract sponsorship for key events during the year including the October Cyber Security Awareness month.

Schedule 1 of the draft legislation provides for the appointment, revocation of appointment and tenure of the Commissioner for Cyber Security.

Schedule 2 of the draft legislation provides for the constitution for Technical Advisory Councils and for the appointment, revocation and code of conduct of members.

PART 3: Objectives and Functions of the Jersey Cyber Security Centre

The Jersey Cyber Security Centre objectives and functions include:

i. Information Security Event Management. This means monitoring threat intelligence (global information on internet and computer activity that may indicate a threat or risk to Jersey), analysing this information, and undertaking a triage process to prioritise it and determine where action is appropriate. This is done in order to prepare, protect or defend the constituency from cyber threats.

ii. Information Security Incident Management. This means receiving intelligence on security incidents and actioning them appropriately. This would include analysis, categorisation and prioritisation of the incident; recommending, supervising, contributing to, or undertaking analysis and forensic analysis of relevant technical artefacts (such as laptops, mobile devices, suspected malware, or internet traffic); recommending or undertaking mitigation and recovery actions, coordinating incident response locally or internationally; and, providing support for crisis management - this could include, for example, advising or undertaking communications with the public or engagement/negotiation with criminal hackers. Please note the provision in the draft legislation for information sharing can be found in Part 6.

iii. Vulnerability Management. A vulnerability is a weakness in an information system that could potentially be exploited. A vulnerability can be technical, process-related, or human behaviour-related. This service would include discovery of vulnerabilities through both proactive research, and through notification by others including security researchers (sometimes referred to as 'hackers') and users of systems. Receipt of vulnerability reports, analysis of vulnerabilities, coordination of response (for example with impacted organisations or technology providers), disclosure of the vulnerability (for example to other CERTs/CSIRTs, the technology providers or national security agencies, or to users of the systems), and response, including recommending and communicating ways to resolve the vulnerability or mitigate the risk.

iv. Situational Awareness. This means building and maintaining a clear picture of global cyber security threats and how these apply to the Jersey Cyber Security Centre's constituency. It includes acquisition of data (for example from news sources, technical data feeds, industry intelligence, national security information, and direct industry engagement); analysis and synthesis of this information to identify actionable insights relevant to Jersey (for example, knowledge of a particular systems vulnerability combined with knowledge of a threat actor using similar vulnerabilities, combined with knowledge that we operate such systems in Jersey, would allow us to predict a threat and address the risk before any impact is felt locally); and communication of this information, both in order to drive immediate behaviours, and to drive longer term change and priorities, for example through the Island-Wide Cyber Risk Assessment or threat specific risk assessments (such as that carried out for Operation Calcite, our response to Russia's invasion of Ukraine)

v. Promote and enable cyber security information sharing amongst organisations to ensure awareness of existing threats, and to provide the ability to take prompt action either on an organisational or Island-wide basis. This may be through provisions to ensure information sharing (for example, incidents affecting operators of essential services which may impact island resilience), or through voluntary information sharing.

vi. Increase the level of cyber resilience across the Island. In collaboration with the of Government of Jersey, Operators of Essential Service and business communities to reduce the risk and impact of major cyber incidents. This may include, for example, provision of support services to relevant organisations (either funded through budget or through cost recovery / cost sharing), setting appropriate standards for cyber security (with the endorsement of Government and through consultation and agreement with relevant competent authorities), through international engagement and cooperation, and through support to boards and stakeholders.

vii. Represent Jersey's cyber security interests locally and internationally, within international cyber security bodies and in dealings with other cyber-attack expertise and response centres. This aligns with the role of the UK National Cyber Security Centre and other national cyber emergency response teams.

viii. Uphold Jersey's cyber security reputation by ensuring Jersey meets the appropriate international standards of best practice for cyber security, and obtaining and maintaining appropriate recognition as a national cyber security agency within the context of a Crown Dependency

ix. Maintain oversight of and report independently on the cyber risk posture of the Island and constituency, for example by undertaking cyber risk assessments for the purposes of Jersey Cyber Security Centre, on behalf of Government of Jersey, and to facilitate Resilience/Emergency Planning.

x. Support and enable effective cyber capability across public services and agencies, for example working with and supporting Regulators, Law Enforcement and Government (through the provision advice, services, expertise and capacity) without prejudice to The Jersey Cyber Security Centre's role as an independent trusted advisor.

The new cyber security legislation will define some of the functions of the Jersey Cyber Security Centre. Namely:

a. monitoring incidents in Jersey; including having the powers to scan publicly accessible networks and systems for malicious activity ('indicators of compromise'), vulnerabilities or configuration errors

b. providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents;

c. responding appropriately to any incident notified to it by any person, including private sector business, government department etc.;

d. providing risk and incident analysis and situational awareness;

e. participating and co-operating in the wider cyber security network;

f. establishing relationships with the private sector in order to facilitate co-operation with that sector;

g. promoting the adoption of and use of common or standardised practices for—

    i. cyber risk management

    ii. cyber security

    iii. incident and risk handling procedures, and

    iv. incident, risk and information classification schemes;

h. co-operating with enforcement authorities to enable the enforcement authorities to fulfil their obligations;

i. facilitate disclose of and receive information from any person if the disclosure is made for the purposes of exercise of any the Jersey Cyber Security Centre's functions;

j. share information as necessary and appropriate with law enforcement, other cyber emergency response teams, and national security bodies, without obtaining permission from data subjects and without restriction as to commercial contracts, as long as it is shared for the purposes of exercise of any the Jersey Cyber Security Centre function;

k. provide or co-ordinate delivery of cyber security services on behalf of local organisations (for example to support shared delivery of security operations, incident response, of vulnerability disclosure services on behalf of multiple organisations);

l. maintain the confidentiality of information, including entering into Memoranda of Understanding (MOU) and data-sharing agreements, and ensuring non-disclosure of information to regulators, government or law enforcement except under court order;

m. for the purposes of the agreed functions - and with the appropriate permission or at the request of the States of Jersey Police, Jersey Office of the Information Commissioner, Jersey Financial Services Commission, or Jersey Competition Regulatory Authority - interrogate computers and networks without liability;

n. only when necessary and appropriate for delivery against the agreed functions, collect and process malware and intelligence including content that may be illegal to access, store or distribute (e.g. accessing dark web);

o. adopt or set guidance and standards in cyber security for Jersey. When setting standards, the Jersey Cyber Security Centre should follow due process and consulate and engage with Government of Jersey and other relevant stakeholders to ensure the standards are recognised, appropriate and proportionate for Jersey.

p. carry out incident readiness and response exercises with participation from public bodies;

q. give the Government of Jersey, telecommunications operators and operators of essential services the right to share information with the Jersey Cyber Security Centre

about cyber security events when this information might otherwise be subject to restriction ; or

r. issue Guidance including general advice to the Minister who can issue Notices (including urgent advice in response to a specific issue or vulnerability).

Through the Commissioner for Cyber Security, the Jersey Cyber Security Centre has the power to set or adopt cyber security standards to help raise the overall cyber resilience of Jersey. There are no enforcement powers associated with this ability. It is the policy intention that any standards would be developed in conjunction with relevant local regulatory bodies. These regulatory bodies would then adopt the standard and be accountable for any enforcement.

PART 4: Operators of Essential Services

In line with many recognised global standards, mandatory reporting of cyber security incidents will be required for those organisations who meet the threshold requires are considered as Operators of Essential Services (OES). The rationale behind this is that these services are considered essential to Jersey. Mandating reporting of cyber incidents will maintain the cyber security resilience of the island.

Operator of an Essential Service (OES) is defined as a person (which includes businesses) or any other service which is essential for the infrastructure of Jersey or the maintenance of critical societal or economic activities in Jersey.

In summary the below sectors are included in the definition:

1. Energy Sector
    a. Electricity subsector
    b. Oil/Crude oil based fuel subsector
    c. Gas subsector
2. Transport Sector
    a. Sea transport subsector
    b. Freight handling subsector
    c. Road transport/ freight distribution subsector
3. Banking and Financial Services
    a. Banking subsector
    b. Financial Services
4. Health Sector
    a. Government of Jersey Medical Services
5. Water Sector
    a. Drinking water supply subsector
6. Digital Infrastructure
    a. Public communications
    b. Digital Service providers
7. Postal and Courier service Sector
    a. Postal services
    b. Couriers services
    c. Couriers of necessary supplies
8. Food Sector
    a. Food production subsector
    b. Food retail subsector
    c. Food distribution
9. Public Administration
    a. Government services
    b. Emergency services

The threshold requirements that determine whether a person (which includes businesses) are classified as an Operator of Essential Services are in Schedule 3 of the draft law.

PART 5: Security Duties on Operators of Essential Services

Reporting a Cyber Security Incident to the Jersey Cyber Security Centre

If an organisation falls into the definition of Operator of Essential Services, then they must report the cyber security incident to the Jersey Cyber Security Centre. As a minimum the information to be reported to the Jersey Cyber Security Centre within the first 48 hours of become aware of the cyber security incident must include the following:

a. the operator's name and the essential services it provides;

b. the time the incident occurred;

c. current status of the incident;

d. the duration of the incident;

e. information concerning the nature and impact of the incident;

f. information concerning any, or any likely, impact of the incident outside Jersey ; and

g. any other information that the OES considers may be helpful to Jersey Cyber Security Centre.

The Jersey Cyber Security Centre shall issue detailed guidance on this prior to the mandatory reporting requirement coming into force.

The law provides for a Ministerial Decision to bring it into force. This allows us to consider possible phasing of mandatory reporting requirements to allow time for OES providers to adjust their incident management processes.

The criteria for a significant incident are outlined in Article 31. It is recognised that the criteria used will impact the volume of incidents that are reportable as well as the value of the information received to JCSC. It is intended that JCSC will produce further guidance to support decision making by OES and that this will build on guidance currently issued in the Jersey Cyber Incident Matrix. An alternative approach would be to define a `significant incident` in Law rather than Guidance, however this may make it difficult to respond effectively to industry feedback and changes in future risks.

Reporting a Cyber Security Incident to the users of a service

Operators of Essential Services are also required to:

a. take such steps as are reasonably and proportionate for the purpose of bringing the relevant information, expressed in clear and plain language, to the attention of persons who use the services who may be adversely affected by the cyber security incident.

b. The relevant information required must include:

   i. the nature of the cyber security incident;
   ii. the technical measures that it may be reasonably practicable for persons who use the essential services to the take for the purposes of
      a. preventing the incident adversely affecting those persons;

b. remedying or mitigating the adverse effect that the security compromise has on those persons; and

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

Enforcement provisions relating to Part 5.

It is the policy intent that JCSC is an advisory and support body. It is also not proposed to give any enforcement powers to any other body. The rationale for this is to give Operators of Essential Services sufficient time to fully understand the requirements being placed upon them by this piece of legislation and adapt accordingly. However, the Government recognises that as risks change in the future, requirements for enforcement may also change, should this be the case, it would be necessary to change the law by Regulation.

Part 4 and Part 5: Operators of Essential Services

Part 4

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

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.

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.

Part 5

4. Do you agree with the mandatory reporting obligations placed on Operators of Essential Services? Please provide your rationale.

5. The Law will mandate an Operator of Essential Service to report a cyber incident within a defined time frame. It is intended that this is a technical notification that can be embedded in the early stages of response processes to alert JCSC to emerging threats, rather than a regulatory notification. Importantly, as JCSC is not a regulatory or law enforcement body and notifications are confidential, there are no potential consequences to the organisation from notification which is designed to make notification as straightforward as possible. This intelligence is most useful within the first 24 hours and its value degrades rapidly with time, however we have also considered that many Jersey OES organisations operate at small scale and therefore a period of up to 48 hours for notification is proposed. We have also considered that regulatory reporting can allow longer periods that reflect the lack of any operational response requirement and the greater certainty needed prior to regulatory filings. For example, the Jersey Office of the Information Commissioner requires breaches to be notified within 72 hours.

   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.

   First choice:

   Second choice:

   Third choice:

   Rationale:

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

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:
    a. immediately alongside the law; or
    b. at a later date?

    If at a later date, please outline which requirement(s) of Part 4 and/or Part 5 you are referring to and the rationale for this, as well as the suggested timeframe.

PART 6: Administrative Provisions

This Part outlines the

1. Offences for providing false or misleading information under the requirement of the draft legislation and
2. Information sharing provisions.

Jersey Cyber Security Centre must protect the information which it gathers and acquires in accordance with the risk posed by such data and must have rules in place governing the security and confidentiality of information, including procedures for access to, and the handling, storage, dissemination and protection of, information.

The Jersey Cyber Security Centre must put in place appropriate measures taking into account available resources and its statutory duties to protect its facilities, information and information technology systems with the purpose of preventing access by those not authorised to do so.

The majority of work that the Jersey Cyber Security Centre will do is in relation to the national security of Jersey. With regards to protecting personal data, Article 41 of the Data Protection (Jersey) Law 2018 provides that processing of personal data necessary for the purposes of safeguarding national security is exempt from data protection principles and the transparency and subject rights provisions of the Law. Therefore, the majority of the duties and functions of the Jersey Cyber Security Centre will be exempt under this Article.

Schedule 1 – Constitution of Jersey Cyber Security Centre

The Commissioner for Cyber Security of the Jersey Cyber Security Centre must be appointed by the Minister for Sustainable Economic Development. The Minister must have regard to the qualifications, experience and necessary skills to perform the role.

The Minister is given the power to vary or terminate the terms of the appointment, in consultation with the Technical Advisory Council.

The Commissioner for Cyber Security is responsible for ensuring the Jersey Cyber Security Centre exercises its functions effectively; proportionally to threats and risks to Jersey from cyber incidents and in accordance with the present international standards on preventing and combating cyber threats, cyber incidents and cyber crime.

The Commissioner for Cyber Security must make reasonable efforts to ensure that the employees of the Jersey Cyber Security Centre maintain high professional standards, are of high integrity and appropriately skilled and trained, and have the appropriate security clearance levels for handling and disseminating sensitive and confidential information.

Schedule 2 Constitution of Technical Advisory Council

The Technical Advisory Council (TAC) will be established to support the Commissioner for Cyber Security with specialist advice as well as input on the work of JCSC.

The primary TAC also has a carefully defined governance role, with an ability to comment independently in JCSC's annual report, and a requirement to be consulted by the Minister prior to any change in the Commissioner. This is designed to provide additional checks and balances without the cost and overhead associated with more expansive governance arrangements.

The Technical Advisory Council must consist of at least 3 and no more than 5 members.

The TAC is appointed by the Minister, who will also decide if they should be voluntary or remunerated. The Commissioner for Cyber Security provides advice to the Minister on appointment of members of the Council.

More than one Technical Advisory Council

In order to maximise opportunities for inclusion and working in partnership with other organisations, it is possible for more than one Technical Advisory Council (TAC) to be set up. This is to provide flexibility for the future. Examples of potential use cases for specialist TACs might be pan-island co-operation, inter-agency working, or responding to emerging risks and opportunities such as those associated with Artificial Intelligence (AI).

Schedule 3 – Essential Services and Threshold Requirements

For each of the listed Sectors, the policy intent has been to identify a clear threshold limit, above which a person (which includes businesses) would be considered an Operator of Essential Service. These limits have been calculated to capture the key businesses in each subsector, that should they suffer a cyber attack would have a significant impact for Jersey. It is not the policy intent to capture all businesses within each sector that operate on Jersey.

It is a primary objective of this consultation to receive feedback from sector experts around these threshold requirements to ensure they are operable and capture the policy intent.

A '*previous financial year'* has been defined as a period of 12 months ending 31 December the previous year to provide a clearly defined reporting period over which measurements of the threshold limits would be applied.

For each subsector, where feasible, numerical threshold limits have been defined to enable easy identification of Operators of Essential services. For some Sectors the threshold limit is referred to as holding a relevant licence or meeting the requirement(s) stipulated in existing Jersey Law.

For reference, a "public communications provider" is defined as:

> *(a) a provider of a public electronic communications network;*
> *(b) a provider of a public electronic communications service; or*
> *(c) a person who makes available facilities that are associated facilities by reference to a public electronic communications network or a public electronic communications service;*

Schedule 3 – Essential Services and Threshold Requirements

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

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.

10. Do you have any other comments on Schedule 3?