THE HON MICHAEL SUKKAR MP

Assistant Treasurer
Minister for Housing
Minister for Homelessness, Social and Community Housing

Ref: MS22-000290

Senator Helen Polley
Chair
Senate Standing Committee for the Scrutiny of Bills
Parliament House
CANBERRA ACT 2600

Dear Senator Helen

I refer to remarks in the Senate Standing Committee for the Scrutiny of Bills (the Committee) *Scrutiny Digest 1 of 2022* concerning the Corporate Collective Investment Vehicle Framework and Other Measures Bill 2021 (the Bill).

Specifically, the Committee has requested my advice as to:

Issue 1: significant matters in delegated legislation

- why it is considered necessary and appropriate to leave the matters outlined in paragraph [1.8] to delegated legislation; and
- whether the bill could be amended to provide at least high-level guidance regarding these matters on the face of the primary legislation.

Issue 2: Henry VIII clause—modification of primary legislation by delegated legislation

- why it is considered necessary and appropriate to allow regulations made under proposed subsection 1243A(1) to modify any provision of proposed Chapter 8B or the *Corporations Act 2001* more generally; and
- whether the bill can be amended to provide at least high-level guidance constraining the scope of this broad modification power, for example, by providing that before the Governor-General makes regulations for the purposes of proposed subsection 1243A(1), the minister must be satisfied that the modifications would be consistent with the objects set out in the bill.

Issue 1: significant matters in delegated legislation

The Corporate Collective Investment Vehicle (CCIV) framework creates a new type of company for funds management in Australia, designed to be an alternative to the commonly used trust-based managed investment scheme.

The regulation-making powers included in this Bill were carefully crafted to provide for appropriate regulatory accompaniment to the CCIV framework to ensure its workability and consistency with the intended objective of the Bill.

While I note that the Committee has generally not considered a desire for administrative flexibility or consistency with existing legislation to be sufficient justification for the inclusion of regulation-making powers, it remains my view that, in the circumstances outlined in the explanatory memorandum, this flexibility is critical to ensuing that the CCIV framework operates as intended. In particular, this is the case for the operation of CCIVs and sub-funds, such as the rules governing the liabilities of a sub-fund, and rules regarding the holding of the assets of a sub-fund. The ability to respond in a timely manner to gaps, ambiguities, or unintended consequences resulting from the application of such rules is essential to the workability of the CCIV framework.

Issue 2: Henry VIII clause—modification of primary legislation by delegated legislation

I note the Committee's concern regarding the inclusion of subsection 1243A(1) of the Bill. However, my view is that this provision, which would allow for regulations to modify the proposed Chapter 8B of the *Corporations Act 2001,* is essential for quickly addressing unforeseen or changing circumstances. Failing to address these circumstances in a timely manner would lead to inappropriate or anomalous outcomes inconsistent with the policy intention of the CCIV framework, or could indeed render make framework unworkable.

The Government has developed the new regulatory framework for CCIVs in close consultation with relevant experts among industry stakeholders, but it remains a new and as yet untested framework. There remains therefore the possibility that the operation of the Bill in practice may produce unintended or unforeseen results. Including this regulation-making power is critical to ensuring timely and targeted adjustments can be implemented if required.

I note that any regulations made under the provisions identified by the Committee will be subject to Parliamentary scrutiny and disallowance procedures.

Regarding the Committee's request that the Bill be amended to provide high-level guidance regarding the matters identified, it is my view that the regulation-making powers as currently set out have been designed appropriately to ensure the CCIV framework operates in accordance with the objects of the Bill. As the Committee will be aware, the Bill has passed both Houses of Parliament as of 10 February 2022 and received the Royal Assent on 22 February 2022.

I trust this information will be of assistance to you.

Yours sincerely

The Hon Michael Sukkar MP

THE HON JASON WOOD MP
ASSISTANT MINISTER FOR CUSTOMS, COMMUNITY SAFETY AND MULTICULTURAL AFFAIRS

Senator Helen Polley
Chair
Standing Committee for the Scrutiny of Bills
Suite 1.111
Parliament House
CANBERRA ACT 2600

Dear Senator

I refer to correspondence dated 21 March 2022 from the Committee Secretary regarding the Senate Standing Committee for the Scrutiny of Bills' consideration of the Criminal Code Amendment (Firearms Trafficking) Bill 2022 (the Bill).

As set out in the Committee's *Scrutiny Digest No. 2 of 2022*, the Committee has requested detailed advice in relation to the proposed significant increases in maximum penalties included in the Bill. I have considered this request and my response is enclosed at **Attachment A**.

I thank the Committee for the opportunity to clarify these matters, and for its important work in considering legislation that is before Parliament.

I trust that the information provided will assist the Committee in its consideration of the Bill.

Yours sincerely

JASON WOOD

28/3/2022

Attachment A

Significant Penalties

The Senate Standing Committee for the Scrutiny of Bills has requested further advice on the justification for the significant penalties that may be imposed under proposed sections 360.2, 360.3, 361. 2 and 361.3 of the *Criminal Code Act 1995*, to be inserted by the Criminal Code Amendment (Firearms Trafficking) Bill 2022 (the Bill), by reference to comparable Commonwealth offences and the requirements outlined in the *Guide to Framing Commonwealth Offences* (the Guide).

The Bill:

- doubles the maximum penalty for individuals convicted of existing commonwealth firearms trafficking offences in the Criminal Code from 10 years imprisonment or a fine of 2,500 penalty units ($550,000) or both, to 20 years imprisonment or a fine of 5,000 penalty units ($1.1 million) or both.
- introduces aggravated firearms trafficking offences to the Criminal Code that carry a maximum penalty of life imprisonment or a fine of 7,500 penalty units ($1.6 million) or both, which will apply where a person traffics 50 or more firearms or firearms parts, or a combination of both.

The Guide

Part 3.1.1 of the Guide provides that a maximum penalty should aim to provide an effective deterrent to the commission of an offence, and should reflect the seriousness of the offence. Further to this, a high maximum penalty is justifiable where there are strong incentives to commit an offence, or where the consequences of committing the offence is particularly dangerous or damaging.

There is considerable financial incentive to engage in firearms trafficking. Firearms are a key enabler for transnational serious and organised crime, and are in high demand among organised crime groups and criminals. The cost of buying firearms in the illicit market is generally higher than in the licit market, generating significant profit for illicit market vendors. In 2018, a joint law enforcement operation between the United States and Australia recovered a number of illegal firearms in Australia which had been purchased on the darknet with Bitcoin. As an indication of the profits available, a handgun that would cost $500 USD in the licit market cost $3,400 USD on a darknet illicit market.

In addition to the financial incentive, a further incentive driving organised groups and criminals to obtain illegal firearms is the absence of any record of being a lawful firearm owner. This can then deflect initial attention of law enforcement in any gun related crimes. There is also the possibility that organised crime groups and criminals can gain a reputational advantage from possessing or having access to a weapons cache.

Firearms trafficking is a serious crime that poses an ongoing and potentially long term threat to the safety of all members of the Australian community. Once in the illicit market, firearms can be accessed by criminals and used in the commission of serious and violent crimes. Illegally trafficked firearms or firearm parts are generally untraceable, can remain within the illicit market for decades and can be used in multiple crimes over their lifespan. They enable organised crime groups to protect their interest and be more lethal in their activities.

The combined effect of increased maximum penalties for existing firearms trafficking offences, as well as the introduction of life imprisonment penalties for the proposed aggravated offences, will provide a strong deterrent against firearms traffickers and their facilitators in organised crime, while reducing the incentives to commit these offences. Additionally, these penalties reflect the community's expectations and the serious consequences of firearm-related crime.

Comparable Commonwealth offences

Comparable offences under the Criminal Code that carry similar maximum penalties to those proposed in respect of the substantive firearms trafficking offences included in the Bill are:

- trafficking marketable quantities of controlled drugs (section 302.3);
- cultivating or selling marketable quantities of controlled plants (section 303.5 and section 304.2 respectively);
- manufacturing marketable quantities of controlled drugs (section 305.4); and
- importing and exporting marketable quantities of border controlled drugs or border controlled plants (section 307.2).

Each of these offences carry a maximum penalty of 25 years imprisonment (five more than proposed for existing firearms trafficking offences), or 5,000 penalty units ($1.1 million) or both.

Additionally, the offences of cultivating commercial quantities of controlled plants (section 303.4), selling commercial quantities of controlled plants (section 304.1), manufacturing commercial quantities of controlled drugs (section 305.3), and importing and exporting commercial quantities of border controlled drugs or border controlled plants (section 307.1) each have penalties of imprisonment for life or 7,500 penalty units, or both. These are in line with the penalty for the proposed aggravated firearms and firearm parts trafficking offence.

The proposed increased maximum penalties for existing firearms trafficking offences, and the proposed penalties for the new aggravated offences, are analogous with the maximum penalties applied to serious drug offences. This indicates the serious social and systemic harms posed by both forms of trafficking and supply. In each case, the offender's behaviour gives rise to harmful and potentially deadly outcomes.

The increased penalties proposed by the Bill would also more closely align the Commonwealth's maximum penalties with maximum penalties for trafficking offences in the States and Territories. For example, in NSW firearms trafficking offences can attract a maximum sentence of 20 years' imprisonment (section 51 *Firearms Act 1996* (NSW)), while in the ACT repeated firearms trafficking offences within a 12-month period can also attract a maximum penalty of 20 years' imprisonment (section 220 *Firearms Act 1996* (ACT)).

THE HON KAREN ANDREWS MP
MINISTER FOR HOME AFFAIRS

Ref No: MS22-000563

Senator Helen Polley
Chair
Senate Standing Committee for the Scrutiny of Bills
Parliament House
CANBERRA ACT 2600

Dear Chair Helen

I refer to the Committee's request, dated 21 March 2022, for further information on the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 1) Bill 2021 (the Bill).

Delegation of powers, functions or duties under proposed section 9D

In Scrutiny Digest 2 of 2022, the Committee requested more detailed advice as to the level of staff members who, in practice, it is expected will be delegated the power to give emergency authorisations under proposed subsections 9D(1)-(3) of Schedule 1 to the Bill.

Due to the sensitive nature of the operational activities involved, I will not comment on the specific levels of staff members who may be delegated the power to give emergency authorisations under proposed subsections 9D(1)-(3).

As I stated in my previous response to the Committee, there is a strong operational need for this power to be devolved to ensure that appropriate decisions can be made quickly where there is an imminent threat to an Australian person's safety. The new emergency authorisation is for the limited scenario in which an immediate or near-immediate response is required. Introducing additional delay into the authorisation process could make the new authorisation framework unworkable and potentially defeat its purpose by putting Australians at further risk. Crucially, the scenario is also limited to where it is reasonable to believe that the Australian person would consent to the production of intelligence about them if they were able to do so.

Overseas staff operate in a variety of contexts, with differing levels of seniority. Officers in the field are often best placed to assess the immediacy of a threat, and the best way to gather intelligence to assist an Australian person whose safety is at risk.

In practice, decisions would likely be made by the most senior officer in the relevant location. However, the level of these officers can differ between locations. The delegation ensures it is possible for suitable individuals in the relevant location and time zone to make decisions if required.

In the unlikely circumstance that the most senior officer is not available, the operational need for approval by a more junior officer to act immediately in a potentially life or death situation, coupled with the need for fast consideration by the agency head and responsible Minister, outweighs any limited risks posed by a more junior staff member being delegated this power in the very limited circumstance where an Australian person is at imminent risk overseas.

On whether Schedule 1 to the Bill should be amended

The Committee also requested more detailed advice as to whether Schedule 1 of the Bill could be amended to require that an agency head, when making a delegation under proposed subsection 9D(14), must be satisfied that the person has the appropriate training, qualifications or experience to appropriately exercise the delegated power.

The requirement that the power be expressly delegated by the agency head in writing, rather than conferred automatically to all, or a class of, agency staff, ensures the agency head will have regard to the appropriateness of the officers being authorised at the time of granting the delegation. In practice, the agency head will only delegate the power to issue emergency authorisations to those officers he or she considers to possess the necessary skills and training to make time critical judgments about the production of intelligence. Further, officers will be required to comply with any written directions given by the agency head when exercising a power, performing a function or discharging a duty under the delegation.

For these reasons, it is not necessary to amend the Bill to include additional decision-making criteria in the proposed delegation power in Schedule 1.

Finally, the Committee requested more detailed advice as to whether Schedule 1 of the Bill could be amended to limit the delegation of an agency head's responsibilities under proposed subsections 9D(4) or (5) to members of the Senior Executive Service.

The responsibilities under proposed subsections 9D(4) and (5) include requirements to notify the responsible Minister, Inspector-General of Intelligence and Security (IGIS), the Attorney-General and the Minister responsible for administering the *Australian Security Intelligence Organisation Act 1979* (the ASIO Minister). These requirements ensure that responsible Ministers maintain visibility, that the IGIS can properly exercise its oversight function, and that the Attorney-General and ASIO Minister are made aware of threats to security.

Requiring these obligations to only be fulfilled by members of the Senior Executive Service (SES) could have the counter-productive effect of delaying provision of the information and documentation to the responsible Minister, IGIS, Attorney-General and ASIO Minister due to SES having a wide remit of responsibilities and significant competing priorities for their time.

Enabling, in appropriate circumstances, non-SES officers to provide these notifications, for example when SES or a senior officer is not available, will maximise opportunities for Ministerial and IGIS oversight, and will ensure that the Attorney-General and the ASIO Minister are made aware of threats to security as soon as possible.

For these reasons it is not necessary or appropriate to amend the Bill to limit certain elements of the delegation power to members of the SES.

I trust this information will be of assistance to the Committee.

Yours sincerely

KAREN ANDREWS

28 / 3 / 2022

THE HON KAREN ANDREWS MP
MINISTER FOR HOME AFFAIRS

Ref No: MC22-013838

Senator Helen Polley
Chair
Senate Standing Committee for the Scrutiny of Bills
scrutiny.sen@aph.gov.au

Dear ~~Senator~~ Helen

I refer to correspondence of 21 March 2022 to my Office from Mr Glenn Ryall, Committee Secretary, on behalf of the Senate Standing Committee for the Scrutiny of Bills, regarding the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (the Bill).

In Scrutiny Digest 2 of 2022, the Committee requested advice as to why it is considered necessary and appropriate to leave certain matters to delegated legislation. I have considered this request, and I am pleased to provide the Committee with additional information in response, enclosed at Attachment A.

I trust that the information provided will assist the Committee in its consideration of the Bill.

Yours sincerely

KAREN ANDREWS

28 / 3 / 2022

RESPONSE TO SENATE STANDING COMMITTEE FOR THE SCRUTINY OF BILLS

SCRUTINY DIGEST 2 OF 2022

Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

Significant matters in delegated legislation

Committee request:

1.153 The committee therefore requests the minister's detailed advice as to why it is considered necessary and appropriate to leave each of the above matters to delegated legislation.

Response:

A disruption to critical infrastructure could have serious implications for business, governments and the community, affecting supply and service continuity, and damaging economic growth.

The reforms in the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (the SLACIP Bill) will uplift the security and resilience of Australia's critical infrastructure by requiring industry to identify and mitigate security risks. These reforms are a key action under Australia's Cyber Security Strategy 2020 and are part of a range of measures the Australian Government is putting in place to strengthen Australia's ability to manage and respond to security risks across critical infrastructure sectors.

The reforms will enhance the security and resilience of Australia's critical infrastructure, in line with the threats posed in the world today and be better prepared to tackle those into the future, by requiring certain responsible entities to adopt and maintain a critical infrastructure risk management program. This will strengthen the resilience of essential services by embedding preparation, prevention and mitigation activities into ongoing business practices.

The regulatory framework that would be established by the SLACIP Bill relies on delegated legislation where necessary to ensure that the statutory framework remains appropriately flexible and adjustable, with a focus on minimising the regulatory impact on entities. With technologies and industries constantly evolving, the proposed rule-making powers in the Bill would enable the Minster to ensure all critical infrastructure assets are included, now and into the future. The rule-making powers provided for in the Bill are essential to ensure the framework is flexible and responsive.

The Government has consulted extensively in the development of this Bill, and will continue to engage across critical infrastructure sectors on the requirements that will underpin the Risk Management Program. Consistent with this approach, and in line with recommendation 9 of the Parliamentary Joint Committee on Intelligence and Security's *Advisory Report on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018* (the PJCIS Advisory Report), the draft *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 22/018) 2022* (the draft Rules) have been included at Attachment C to the SLACIP Bill's Explanatory Memorandum.

Following commencement of the amendments in the Bill, the Minister would be required to undertake a period of mandatory consultation of no less than 28 days on the proposed draft rules. The Minister will consider any submissions and may then choose to make a rule that will commence at a time of my choosing following mandatory consultation. This will allow the obligation to apply only to those sectors without appropriate existing Commonwealth regulations to ensure implementation does not impose any unnecessary burden.

Relevantly, the Minister is not permitted, when making rules, to exceed the principles set out in the primary legislation, and all rules are appropriately subject to parliamentary scrutiny and disallowance.

Additional comments specific to each of the matters identified by the Committee at paragraph 1.150 of Digest 2 of 2022 are set out below, for the Committee's consideration.

...amend section 5 to repeal and replace the definition of 'data storage or processing service' and provide that this can include a service specified in the rules and that the rules may also prescribe that a service is not a data storage or processing service

In line with recommendation 7 of the PJCIS Advisory Report, the definition of 'data storage or processing service' in the Bill has been informed by extensive consultation across sectors, to ensure it appropriately captures relevant assets. Paragraphs (a) and (b) of the definition provide for certain services expressly in the legislation; however, it is necessary to include a rule-making power alongside this to ensure that the framework is sufficiently flexible to encompass future developments in relation to data storage and processing services, and to incorporate services that are not already covered by paragraphs (a) and (b) but might be identified in the course of ongoing consultation with stakeholders after the amendments in the SLACIP Bill are enacted.

As noted at paragraph 43 of the Bill's Explanatory Memorandum, the rule-making power in paragraph (c) of the new definition of 'data storage or processing service' will allow the Minister to make rules specifying additional services as data storage or processing services to ensure that technical advancements in this field, which are occurring rapidly, can also be appropriately included in the scope of the definition.

Relevantly, the new definition also provides that the rules may prescribe that a specified service is not a 'data storage or processing service'. This provides for the Minister to carve-out a service from the scope of the definition, if required.

...amend section 8 to provide an exemption to when an entity will be a direct interest holder in circumstances specified in the rules

The *Security of Critical Infrastructure Act 2018* (SOCI Act) currently exempts moneylenders from responsibilities under the legislation, in circumstances where that moneylender or the custodial or depository services are not in a position to influence or control a critical infrastructure asset.

However, consultation on the reforms has revealed that there is a risk that the current provision does not operate as intended – that is, for the moneylenders and custodial or depository services exemption to only apply prior to a moneylender and custodial or depository services enforcing a security over the critical infrastructure assets and thereby gaining influence or control over that asset. In those circumstances, it is considered appropriate that a moneylender or custodial or depository services should be treated the same as any other direct interest holder.

The SLACIP Bill will ensure that the moneylenders and custodial or depository services exemptions operates as originally intended. Consultation on the reforms has also revealed that custodial services and other similar entities should also be exempt from responsibilities under the legislation where those entities are in a position to directly or indirectly influence or control a critical infrastructure asset. The SLACIP Bill therefore includes a new rule-making power to future-proof the legislation and provide the Minister with sufficient flexibility to respond to developments in this area of law.

...amend section 12KA to provide that the rules may prescribe specified assets that are critical to the administration of an Australian domain name system or requirements for an asset to be critical to the administration of an Australian domain name system

An asset is a 'critical domain name system' under section 12KA of the SOCI Act where it meets the following criteria:

- the asset is managed by an entity that is that is critical to the administration of an Australian domain name system (see subsection 12KA(2) and section 16 of the *Security of Critical Infrastructure (Definitions) Rules 2021* (the Definitions Rules)): paragraph (1)(a) of the definition; and
- the asset is used in connection with an Australian domain name system: paragraph (1)(b) of the definition.

As noted at paragraph 117 of the Bill's Explanatory Memorandum, this amendment follows consultation with .au Domain Administration Limited (auDA), the entity responsible for the administration of the '.au' country code Top Level Domain, and the Department of Infrastructure, Regional Development, Transport and Communications. These entities raised concerns that the construction of the current definition may capture irrelevant assets used in connection with the administration of an Australian domain name system (e.g. accounting software or event management systems).

In this context, the purpose of the new rule-making power in the SLACIP Bill is to provide greater certainty on what assets are 'critical to the administration of an Australian domain name system'. A rule-making power currently exists under subsection 12KA(2) of the SOCI Act to prescribe the entities that are critical to the administration of an Australian domain name system. Section 16 of the Definitions Rules currently prescribe Domain Administration Ltd (ABN 38 079 009 340) and the entity that administers the '.au' country code Top Level Domain for this purpose.
116. With the amendment to section 12KA in the SLACIP Bill, an asset used by these entities in connection with an Australian domain name system will need to be prescribed in rules made by the Minister to be a critical domain name system.

...insert proposed section 30AB to provide that Part 2A of the bill applies to assets specified in the rules and that the rules may exempt assets from Part 2A for a certain period of time

Proposed section 30AB allows for a nuanced, sector- or asset-specific approach to be taken to the application of the obligations contained in new Part 2A. In determining whether to make rules to apply the obligations to certain critical infrastructure assets, the Minister is likely to consider whether any existing requirements or arrangements appropriately deliver the same outcomes as intended by the critical infrastructure risk management program.

The assets that are critical education assets are an example of a class of critical infrastructure asset with appropriate regulatory requirements or arrangements in place. The Australian Government and Australia's higher education providers have jointly formed the University Foreign Interference Taskforce (UFIT) to enhance safeguards against the risk of foreign interference. The UFIT will deliver the same outcomes as intended by the critical infrastructure risk management program obligation for critical education assets. The Government does not intend to 'switch on' any of the positive security obligations (including Part 2A) for critical education assets.

As noted at paragraph 135 of the Explanatory Memorandum, this reflects the range of regulatory obligations that already exist in relation to some classes of critical infrastructure assets, and the obligations that may exist in relation to future critical infrastructure assets that are identified, and the Government's commitment to avoid duplicating regulation. In the event that any of these alternative regulatory regimes were to be found wanting, the Government will reserve the ability to 'switch on' any or all of the positive security obligations, including the critical infrastructure risk management program (Part 2A), to address any gaps and ensure that entities are subject to suitable and reasonable regulation.

...insert proposed section 30AH, which leaves a number of elements in relation to critical infrastructure risk management programs to the rules

Proposed section 30AH would define the requirements for a critical infrastructure risk management program. Adoption and compliance with a critical infrastructure risk management program will ensure responsible entities have a comprehensive understanding of the threat environment, and develop processes and procedures to respond effectively to the risk of any hazard impacting the availability, confidentiality, reliability and integrity of their asset. This is central to the reforms proposed in the SLACIP Bill.

Under proposed paragraph 30AH(1)(c), the critical infrastructure risk management program must comply with any requirements specified in rules made by the Minister under section 61 of the SOCI Act. Any such rules will be a legislative instrument, appropriately subject to parliamentary scrutiny, and publically available on the Federal Register of Legislation (https://www.legislation.gov.au).

The rules will be used to provide further requirements on how the principles based obligations set out in subparagraphs (1)(b)(i)-(iii) are to be implemented. Given the array of critical infrastructure assets that may be subject to the obligation to adopt and maintain a critical infrastructure risk management program, now and into the future, this mechanism will be crucial for ensuring the program is implemented in a risk-based and proportionate manner while still achieving the desired security outcomes and avoiding any unnecessary burden.

Importantly, proposed subsections 30AH(2)-(12) provide further clarity as to the scope of the rule-making power. The rules may be of general application or may relate to one or more specified critical infrastructure assets, allowing appropriately for a flexible, nuanced approach (subsection 30AH(2)). It is also important to note that proposed subsection 30AH(6) sets out factors the Minister must have regard to in specifying rules under proposed subsection 30AH)1)(c). This would ensure that any rules made for the purposes of the critical infrastructure risk management program are appropriate in all the circumstances, while avoiding unnecessary duplication and regulatory burden for responsible entities.

...insert proposed section 30AKA which provides that entities must have regard to matters set out in the rules when determining to adopt, review or vary a critical infrastructure risk management program

As noted at paragraph 237 of the Explanatory Memorandum, a key theme of the information received from industry stakeholders during consultation was that the critical infrastructure risk management program obligation needs to be flexible and adaptable to the business processes and environment of an individual responsible entity.

In this context, it is appropriate that proposed section 30AKA provides for matters relevant to adopting, reviewing or varying a critical infrastructure risk management program to be set out in the rules.

Proposed subsection 30AKA(7) provides that rules made for subsections 30AKA(1), (3) or (5) may be of general application, or relate to one or more specified critical infrastructure assets. These provisions would allow for varying matters to be specified for different types of critical infrastructure assets and industry sectors.

The amendments in the SLACIP Bill dealing with the critical infrastructure risk management program would require responsible entities of critical infrastructure assets to adopt and maintain a written critical infrastructure risk management program. This is intended to uplift core security practices in relation to the management of critical infrastructure assets by ensuring responsible entities take a holistic and proactive approach toward identifying, preventing and mitigating risks from all hazards.

The Department has worked closely with industry to develop sector-agnostic, principles-based rules which will provide guidance for developing risk management programs, and the specific risks and hazards that should be considered. Where possible, the requirements under the risk management program would recognise or build on existing regulatory frameworks, seeking to minimise the regulatory burden on industry. This would ensure that if an existing regulation already exceeds the relevant risk management program requirement, there is not a duplicative set of obligations in place. This approach reflects clear feedback from industry that the responsible entity is best placed to understand the risks to an asset, and to develop appropriate risk practices.

Importantly, proposed section 30AKA does not act to limit the matters to which the responsible entity may have regard – and that the matters an entity may have regard when adopting, reviewing or varying a critical infrastructure risk management program are not restricted to matters specified in the rules.

…require that incident response plans, cyber security exercises, evaluation reports and vulnerability assessments all comply with requirements set out in the rules

There are four different legislative mechanisms that would implement the enhanced cyber security obligations outlined in proposed Part 2C of the SOCI Act, as provided for in the SLACIP Bill:

- incident response planning obligations (proposed Division 2 of Part 2C),
- cyber security exercises (proposed Division 3);
- vulnerability assessments (proposed Division 4); and
- access to system information (proposed Division 5).