Locked Bag 14051
Melbourne City Mail Centre
Victoria 8001 Australia
T: 1300 360 795
www.ausnetservices.com.au

27 November 2020

Department of Home Affairs
Australian Government

via: web submission

Submission – Exposure Draft of Security Legislation Amendment (Critical Infrastructure) Bill

AusNet Services Ltd together with its subsidiaries, (**AusNet Services Group** or **Group**) welcomes the opportunity to provide a confidential submission to the Department of Home Affairs (**Department**) in response to the Exposure Draft Security Legislation Amendment (Critical Infrastructure) Bill (**Draft Bill**) and Intelligence Services Regulations (together, the **SCI Amendments**).

The AusNet Services Group operates Victoria's primary electricity transmission network, as well as an electricity distribution network and a gas distribution network in Victoria. The Group, also operates certain telecommunications assets, including a network of poles, towers and cables as part of operating its networks and providing connection and metering services to customers in reliance of exemptions under Division 2 of Part 3, and Division 3 of Part 4, of the *Telecommunications Act 1997* (***Telco Act***)). Redundant capacity on these assets is also used by broadcasters and telecommunications companies, as well as other exempt network users.

The AusNet Services Group places great importance on ensuring the security of our networks and appreciates the policy considerations behind the SCI Amendments. However, there are some areas of the SCI Amendments where we consider that greater certainty, or closer alignment with existing standards in Australia and overseas, would assist the AusNet Services Group, and other impacted asset owners and operators, with implementing security measures effectively.

Our key proposals, which are set out in more detail in our attached submission, are summarised below. The purpose of our proposals is to avoid misalignment and complexity, allowing organisations to focus on ensuring they have robust capabilities and processes rather than focussing on formal compliance.

1 **Inconsistency with Existing Obligations:** There is a risk of obligations under the Draft Bill being inconsistent with existing obligations under energy-sector laws, regulations and rules, many of which operate at the State and Territory level. In order to avoid entities being subject to competing obligations, the Draft Bill should include anti-overlap provisions, and the Department should engage with State and Territory governments to determine whether corresponding provisions are required in their respective laws, regulations and rules.

2 **Immunity from Liability:** The immunity from damages provisions in sections 30BE, 35AAB and 35AW are insufficient. We propose that:

(a) the Draft Bill be amended so that the immunities extend to non-damage based remedies, statutory liability and other adverse regulatory outcomes;

(b) immunities should also apply in respect of the Australian Signals Directorate's (**ASD's**) step-in powers (section 35AX) and enhanced cyber security obligations (Part 2C);

(c) the Department consider whether regulated entities should be entitled to recover from the ASD where its exercise of step-in rights causes loss; and

(d) the Department engage with State and Territory governments to ensure that existing laws do not cut across immunities in the Draft Bill.

3 **Notification of Cyber Security Incidents:** The timeframes and thresholds under the Draft Bill for notification of cyber security incidents are shorter and lower than for incident notification obligations under comparable overseas and Australian regimes. Only the obligation proposed in section 30BC (for incidents with a 'significant impact' on a critical infrastructure asset) should apply, and the obligation in section 30BD should be removed. In addition, the timeframe for notification should be extended to 72 hours to align with comparable security obligations.

4 **Timeframe for Implementation:** The Draft Bill should allow for staggered implementation of the relevant obligations (particularly the positive security obligations), to accommodate longer lead-in times that may be required to properly implement more prescriptive obligations. This could be achieved by including language in clauses 18A, 30AB and 30BB which provides that the relevant obligations will commence in accordance with an implementation timetable specified in the rules.

5 **Cost of Implementation:** In order to assist entities with managing the cost of implementing their new obligations, amendments to the Draft Bill should be made that allow the Department to exclude entities that operate critical infrastructure assets in multiple classes from certain obligations in the interests of avoiding duplication of their obligations. In addition, the rules should provide appropriate synergies to achieve this outcome. We also note that to the extent possible, early sharing of information about the nature and extent of obligations will assist entities in the energy-sector (and other price-regulated sectors) with determining their pricing models and, where applicable, pass through applications.

6 **Multiple use assets:** As drafted, it is possible for the Group's telecommunications network to be classed as both a critical electricity asset (owned/operated by the Group) and a critical telecommunications asset. The result of this is that the Group's telecommunications network could be caught under separate obligations attaching to two (or more) distinct entities. The Rules should make clear that network units (as defined under the *Telecommunications Act 1997* (Cth) (**Telco Act**)) which are the subject of exemptions under Division 2 of Part 3, or Division 3 of Part 4, of the Telco Act, and which otherwise form part of a critical infrastructure asset, are not critical telecommunications assets.

7 **Intelligence Sharing:** The Draft Bill should include a provision that facilitates the two-way sharing of intelligence information to align with the objectives of the Cyber Security Strategy 2020.

We would be pleased to meet with you or your team to talk further about our current practice or to discuss any of our responses in further detail.

If you would like to arrange a meeting or otherwise discuss any of the issues we have raised, please do not hesitate to contact Naomi Kelly, EGM Governance, General Counsel and Company Secretary ([redacted] or [redacted]) of my team in the first instance.

Sincerely,

[redacted]

Tony Narvaez
Managing Director
AusNet Services

SUBMISSION IN RESPONSES TO THE SCI AMENDMENTS

The object of our proposals is to ensure that the security measures required under the SCI Amendments will be effective. Effectiveness requires a framework that can be implemented holistically and cost-effectively, which avoids inconsistency and unnecessary duplication and which encourages compliance by affording sufficient protections to regulated entities in respect of their compliance activities.

Subject	Concern with current proposal	AusNet Services proposal
Inconsistency with Existing Obligations	The electricity and gas industries are highly regulated with a range of obligations imposed by legislation, regulations, licenses, directions, governmental orders and other regulatory instruments, largely at the State and Territory level. For example, the National Electricity Market is supported by national laws and rules, adopted by the participating States and Territories and safety, emergency and industry regulation is primarily based on distinct State and Territory laws. On the whole, these regulations are aimed at promoting investment in, and efficient operation and use of, electricity and gas services for the long term interests of consumers with respect to price, quality, safety, reliability and security of supply. Given this, the development of the Draft Bill and the rules to be made under it must take account of these obligations to ensure there are no material conflicts or overlaps with the existing regulatory regimes. Where the potential for conflicts or overlaps exists, arrangements must be put in place to manage such conflicts or overlaps – either by recognition of such in the Draft Bill or in the conflicting regulations. Without the benefit of the sector-specific rules or directions that are proposed to be made under the Draft Bill, it is difficult to point to specific examples of conflict or overlap. However, the power given to the Australian Signals Directorate (**ASD**) to interfere with a relevant entity's operations via step-in (sections 35AC	The Draft Bill should include anti-overlap provisions which seek to resolve the potential for conflict and overlap with existing and future industry legislation, regulations, licenses, directions, governmental orders and other regulatory instruments. The Department should also engage with State and Territory regulators to determine whether corresponding anti-overlap provisions are required in their respective laws, regulations and rules.

Subject	Concern with current proposal	AusNet Services proposal
	and 35AX) and the Minister's powers to give directions to relevant entities (sections 35AB and 35AQ) may, for example, conflict with: • AEMO's directions powers under the National Electricity Law and National Electricity Rules; • prospective powers to impose Ministerial licence conditions;[1] and • the powers and discretions provided under various emergency, industry and safety legislation in the State of Victoria.[2] Clarity about the resolution of such potential conflicts is imperative. AusNet Services' view is that the relevant obligations under the Draft Bill should not go live until such conflicts have been expressly addressed in relevant legislation. The Constitutional implications of potential conflicts and inconsistencies between the federal Draft Bill and existing State- and Territory-based electricity regulations must also be considered. The existing provisions in sections 16 and 17 of the SCI Act do not clarify how such inconsistency would be dealt with and it may not necessarily be an issue that would be addressed by the operation of section 109 of the *Constitution*. The operation of section 109 of the *Constitution* may also not be an appropriate or effective solution.	

[1] Energy Legislation Amendment (Licence Conditions) Bill 2020 (Vic).
[2] Examples include Section 141 of *Electricity Safety Act 1998* (Vic), Part 6 of the *Electricity Industry Act 2000* (Vic), *Emergency Management Act 2013* (Vic), Part 7A

Immunity from Liability	The Draft Bill affords limited protections for an entity's good faith compliance with notification obligations (section 30BE), and directions by the Minister or ASD (sections 35AAB and 35AW). There are four key issues with the current approach. First, the provisions in the Draft Bill only protect entities from liability for damages. They do not protect an entity from the following adverse outcomes: • **Any non-damage based remedies under contract or in equity**: e.g. service level payment or annuity reduction may be payable under a contract with a network customer and/or that customer may have termination rights depending on the consequence of the direction or intervention. • **Liability under another statute, regulation or rule**: e.g. if a direction issued to an entity under the Draft Bill were to prevent such entity from complying with a direction made by AEMO under the National Electricity Rules then the entity may be liable to pay a civil penalty for breach of rule 4.8.9A of the National Electricity Rules. • **Other regulatory consequences** to which an entity may be subject that do not amount to civil penalties: these may include guaranteed service level payments, reductions in maximum allowable revenue or penalties payable under expenditure and other incentive schemes as a result of its compliance with a direction or intervention. The second issue is that the protections in the Draft Bill only apply in limited circumstances, and do not cover the field of circumstances in which an entity's compliance with the Draft Bill could lead to adverse outcomes. In particular, there is no protection for an entity in relation to:	The following changes to the immunity position in the Draft Bill would help resolve current legal issues and encourage compliance. The existing immunity provisions in clauses 30BE, 35AAB and 35AW of the Draft Bill should be expanded to protect parties from a broader range of potential claims, losses and damages than 'damages'. The immunities should protect parties from exposure to civil penalties under legislation, contractual and common law remedies (including but not limited to damages), and other adverse outcomes under regulated revenue regimes and regulatory or contractual service level regimes. Other legislation in the energy sector provides for broader immunities than those proposed in the Draft Bill. For example, section 119 of the *National Electricity Law* or section 99 of the *Electricity Industry Act 2000* (Vic), which provides that: "A person acting in good faith in the execution of this Part or any proclamation or direction under this Part is not liable to any action, claim or demand on account of any damage, loss or injury sustained or alleged to be sustained because of the operation of this Part or of any thing done or purporting to be done under this Part or any proclamation or direction under this Part."

	• acts or omissions by the ASD while it is exercising its step-in powers under section 35AX; or • compliance with enhanced cyber security obligations under Part 2C, such as conducting required cyber security exercises or providing access to system information, should those obligations apply. The third, related issue is that an entity has no recourse against ASD for damage that its step-in or access to information may cause to such entity (such as damage to IT systems, loss of data or loss of revenue) due to the exclusion of the ASD's liability in section 35BF. In the absence of a right of recovery, this risk of loss may also have insurance implications for the Group. Finally, as noted above in relation to potential inconsistency, any immunity implemented under the Draft Bill from State or Territory legislative payment, penalties or incentives would need to be Constitutionally sound, in order to ensure that the immunity has the intended effect.	While adopting these examples would not address all of the issues with the immunities provided in the Draft Bill, they serve to illustrate that in each particular context, the scope and content of immunities requires careful consideration and analysis (including from a jurisdictional / head of power perspective) to ensure that appropriate and effective protections, that encourage compliance and co-operation are implemented. Similarly, broad immunities should be included in respect of the step-in powers under section 35AX and enhanced cyber security obligations under Part 2C of the Draft Bill. The Department should also consider whether it is appropriate for regulated entities to be able to recover certain costs from the ASD where its exercise of step-in rights causes damage. Alternatively, the Department should consider the insurance and cost implications if this risk is not addressed. To ensure the immunities in the Draft Bill operate effectively, the Department may need to coordinate with State and Territory governments to include corresponding provisions in laws that may contain obligations inconsistent with those under the Draft Bill.

Subject	Concern with current proposal	AusNet Services proposal
Notification of Cyber Security Incidents	The obligation to report cyber security incidents has an unusually short timeframe and is triggered by a relatively low threshold. This is out of step with existing incident notification obligations in Australia and overseas. **Timeframe:** The ASD or prescribed regulator must be notified of an incident 'as soon as practicable' and within 24 hours of AusNet Services Group becoming aware that an incident has a 'relevant impact' on a critical infrastructure asset (section 30BD), or within 12 hours of becoming aware that it has a 'significant impact' (section 30BC). We note that under similar legislation in the UK (made under the EU's NIS Directive),[3] notification must occur 'without undue delay' and within 72 hours. This also aligns with reporting requirements under the General Data Protection Regulation (**GDPR**), as well as analogous Australian information security regimes like CPS 234. **Threshold:** The lower notification threshold in section 30BD requires notification within 24 hours even for an 'imminent' incident that 'is likely to have' any impact on the availability, integrity, reliability or confidentiality of the relevant asset. This is a very low threshold that would impose a disproportionate, operationally onerous obligation. This is contrasted with the position under UK law, which only requires notification of incidents with a "significant impact on the continuity of essential services", or CPS 234, which has a materiality threshold. The threshold in section 30BC is for incidents with a 'significant impact' which aligns more closely with the UK position.	Only the obligation proposed in section 30BC (which arises for incidents with a 'significant impact' on a critical infrastructure asset) should apply, and the obligation in section 30BD should be removed. The timeframe for notification in section 30BC(1)(d) should be extended from 12 to 72 hours to align with comparable security obligations under CPS 234 and the EU's NIS Directive. In addition, further clarification should be provided in the Draft Bill of when 'awareness' that an incident meets the relevant thresholds will arise.

[3] *The Network and Information Systems Regulations 2018* (UK) s 11(3)(b)(i).

Timeframe for Implementation	The Department has previously indicated (in its Energy Sector Workshop on 20 August) that obligations are intended to come into effect in mid-2021. It is not clear whether the initial implementation will include switching on positive security obligations, nor will the exact content of those obligations be known until it is specified in the rules. It is conceivable that the rules may include a series of prescriptive obligations to be taken, the implementation of which will require some time. Depending on the nature of the obligations imposed, there may be a need to stagger implementation of particular requirements (taking into account whether implementation would have a long lead-time). A staggered approach to implementation would be consistent with what has occurred in other contexts. For example, the Australian Prudential Regulatory Authority, in respect of the implementation of Prudential Standard CPS 234 (Information Security), staggered the implementation of obligations in relation to third parties, and where relevant, granted extensions to the timing of obligations. Alternatively, a similar outcome could be achieved by way of an enforcement "grace period". The relevant regulator would also have the flexibility to grant extensions for compliance with certain obligations (provided organisations demonstrate a roadmap to compliance), as appropriate. However, this approach is less certain and less preferable. We note that the implementation of the Security of Network and Information Systems (**NIS**) directive in the EU has been staggered. In the UK, for example, the regime was implemented after a year-long assessment process aimed at identifying threats and vulnerabilities, followed by a stepped approached to enforcement in which penalties were the last resort (see page 18 of the UK's NIS Implementation Guidance).	The Draft Bill should include language that allows the Department or relevant regulator flexibility to determine when Positive Security Obligations are implemented. This could be achieved by including language in sections 18A, 30AB and 30BB which provides that the relevant Part will commence in accordance with the implementation timetable specified in the rules.

Subject	Concern with current proposal	AusNet Services proposal
Cost of Implementation	Compliance with the SCI Amendments will cause regulated entities to incur additional cost, part of which will be borne by consumers. In the energy sector, any increase in utility bills should be minimised. There are three key aspects of the SCI Amendments that have the potential to drive the cost of implementation: (a) **Duplication**: AusNet Services Group could be subject to separate rules in respect of the energy transmission, energy distribution, gas distribution and telecommunication assets it operates – the Group is not the only entity which will be responsible for more than one critical infrastructure asset. This could result in duplication of obligations (e.g. obligations to report incidents to different sector regulators or the ASD) or inconsistency (e.g. different requirements for critical infrastructure risk management program in respect of the different asset classes). Although the Department has indicated in its Explanatory Document that the rules will seek to avoid this, the issue is not currently addressed in the Draft Bill. Section 12L of the Draft Bill only allows the Department to specify *additional* responsible entities in the rules, but does not allow the *exclusion* of entities. (b) **Lack of knowledge**: An Entity cannot accurately predict the cost of implementation until they know the full nature and extent of its obligations under the rules. As a price-regulated business, AusNet Services Group cannot pass through its compliance costs in the same way as entities in other sectors. For this reason, entities like AusNet Services Group will require information as early as possible in order for additional costs to be factored into revised regulated pricing proposals or pass through applications, where applicable.	We recommend that the following measures be implemented to mitigate the cost impact of the reforms: (a) The Draft Bill should include an anti-overlap provision which states that if an entity is subject to obligations in respect of one critical infrastructure asset class, it is not capable of being captured in respect of another asset class unless otherwise specified in the rules. Alternatively, the rules should, to the extent possible, be prepared so as to provide appropriate synergies for entities which operate multiple critical infrastructure assets across various sectors. (b) A new provision should be added to section 12L of the Draft Bill which states that the rules may specify that a particular entity is *not* a 'responsible entity' for a particular critical infrastructure asset. This would mirror the existing power to exclude critical infrastructure assets under section 9(2). (c) Information about the extent and timing of obligations should be shared as early as possible. This will enable relevant information

Subject	Concern with current proposal	AusNet Services proposal
	(c) **Aggressive timeframe**: The tight timeframe proposed by the Department (with obligations to commence in mid-2021) will lead to increased cost, including due to operational difficulties in meeting that timeframe. A short timeframe could also constrain the availability of any technical consultants necessary to help responsible entities prepare for commencement, which could lead to increased cost or difficulty with achieving compliance within the required timeframe.	to be factored into pricing submissions for regulated entities like AusNet Services Group. (d) A provision allowing for staggered implementation of obligations should be included in the Draft Bill.
Multiple use assets	The AusNet Services Group, like a number of similar transmission and distribution companies, owns and operates a telecommunications network which is a key element of its electricity networks. The Group takes the benefit of certain exemptions under the Telco Act from holding a carrier licence (see Part 3 Division 2 of the Telco Act) and from being classed as a *carriage service provider* (see Part 4 Division 3 of the Telco Act). These exemptions enable the Group to operate its networks and provide connection services to customers, as to make available excess capacity on its telecommunications network to licensed carriers (and other exempt entities). For example, because the Group's telecommunications network forms an intrinsic, and inseparable, part of the Group's electricity networks, the telecommunications network would likely be caught by the definition of critical electricity asset. It is possible, however, that the telecommunication network may also be classed as a critical telecommunications asset by virtue of the fact that part of the Group's network is connected to, and forms part of, the telecommunications network which is owned/operated by those licensed carriers who use the Group's excess capacity. In addition, the Group's telecommunications network could also be otherwise classified (depending on	Pursuant to section 9 of the Draft Bill, the Minister should prescribe that network units (as that term is defined in the Telco Act): (a) which are the subject of exemptions under Division 2 of Part 3 of the Telco Act; and (b) which otherwise form part of a critical infrastructure asset, are not critical telecommunications assets or critical infrastructure assets that relate to the communications sector.

Subject	Concern with current proposal	AusNet Services proposal
	the rules that are established) as critical infrastructure assets that relate to the communications sector. This is due to the way in which telecommunications network is defined under the Telco Act (and which is adopted under the Draft Bill). The result of this is that the Group's telecommunications network could be caught under separate obligations under the Draft Bill, that may attach to two (or more) distinct entities – the Group and the licensed carrier. This gives rise to a number of issues, including those relating to inconsistency and immunity as set out above. The Group strongly considers that its assets should fall under one class of critical infrastructure asset only.	
Intelligence Sharing	The Draft Bill only provides for the sharing of security information and intelligence by regulated entities to government bodies and regulators. This does not reflect the two-way intelligence sharing arrangements that were put forward in the Government's Cyber Security Strategy 2020, which emphasised that the Government would "improve threat information sharing with industry", and noted that "successful threat information sharing is measured by an increased two-way flow of cyber security information". Access to such threat information would strengthen industry partnerships in line with the Government's Cyber Security Strategy 2020, and provide businesses with access to threat information that would allow them to better prepare for and defend against cyber threats, and coordinate with emergency planning of AEMO or State and Territory regulators.	The Draft Bill should include a provision that facilitates the ASD, the Department or the relevant industry regulator to share information with responsible entities in relation to their critical infrastructure sector(s).