Submission in response to consultation by the Department of Home Affairs on:

Protecting critical infrastructure and systems of national significance

September 2020

EXECUTIVE SUMMARY

1. Optus welcomes the opportunity to provide comment on the proposed new regulatory arrangements outlined in the consultation paper 'Protecting critical Infrastructure and systems of national significance' (August 2020). The new regulatory regime is likely to have a significant effect on Optus' existing operations.

2. The SingTel Optus Pty Ltd group of companies ("Optus") own and operate significant national telecommunications infrastructure and supply carriage and content services to a large portion of the Australian community. Optus acknowledges the onus this creates to serve its customers and the community with competitive and secure services, and it takes this responsibility seriously.

3. Optus controls entities which are carriers, carriage services providers and content services providers and which operate in several of the proposed regulated sectors.

4. Optus agrees it should be a shared national endeavour between Government and critical infrastructure providers to increase the security and resilience of infrastructure critical to Australia's economic well-being**.**

5. Optus recommends that the legislative imposition of the new critical infrastructure security policy to the communications sector is primarily via changes to the Telecommunications Act in concert with the proposed new parts of Security of Critical Infrastructure Act.

6. The proposed new critical infrastructure security laws are likely to add to the currently high commercial stresses on the communications industry unless Government looks both within the proposed new framework, and also the other policy settings within its control, to moderate adverse impacts on incentives to investment, limit compliance costs and avoid crowding-out legitimate commercial endeavour.

7. Government efforts to build the security posture of critical infrastructure should be designed to work co-operatively, or at least co-exist without damaging existing commercial activities also seeking to promote security outcomes for Australian business.

8. The definition of critical infrastructure in a communications network context should focus on the core network elements, those elements which contain the real intelligence of the network and which in practice exercise the command and control functions critical to the proper functioning of the network.

9. Optus recommends that the task of mapping of potential critical infrastructure entities to the three regulated categories (critical infrastructure provider, regulated critical infrastructure provider and systems of national significance) be delegated by legislation to a subsequent process with suitable checks and balances**.**

10. Optus recommends that the scope of regulation be defined by the cross section of an entity definition and asset definition:

    (a) The regulated entity - which owns and operates defined critical infrastructure assets;
    (b) The defined critical infrastructure (e.g. core network assets) owned by the regulated entity; and
    (c) Excludes business activities and assets which are not directly related to the critical infrastructure assets or activities.

11. Optus acknowledges the high-level principles set out in the description of Initiative 1 in the consultation paper form a suitable generic framework of for the development of the Positive Security Obligation and guiding risk management and governance arrangements for regulated entities.

12. The proposed new sectoral security standards should adopt a risk-based approach, and the process and decision-making criteria to determine the standards should have suitable checks and balances.

13. Optus recommends that the Department of Home Affairs accept that the information released to date via the consultation process does not provide a reasonable basis for entities or sectors to contribute quantitative information to a cost-benefit analysis or regulatory impact assessment of the proposed framework**.**

14. Optus considers that vital details of the future state of the positive security obligation are not yet available and hence a quantitative cost analysis cannot be undertaken of the impact of the obligation on regulated entities**.**

15. Optus anticipates that compliance arrangements triggered by the proposed new regulatory obligations will have cost, employment and process impacts, in both the short and the long term, across all major categories of corporate activity involved in managing its carrier or carriage service provider business operations.

16. Optus recommends the legislation provides adequate time for designing and implementing each of the key components of the framework (e.g. sector specific security standards and compliance checks against those standards) because the integrity of this important work should not be compromised by artificially tight deadlines.

17. Optus considers it important for legislation to describe a regulatory policy intent that the new security law be administered by regulators which function co-operatively with regulated entities, and that they have a mandate to operate with a 'light touch' regulatory ethos. It is reasonable for the Critical Infrastructure Centre within the Department of Home Affairs to be assigned the role as regulator of the communication sector under the new framework.

18. Optus is concerned that the overall net effect of the series of proposed new information exchange processes could impose undue bureaucratic burden (cost and process) on regulated entities.

19. Optus supports the policy vision that improved situational awareness, including the development of a near real-time national threat picture, is an appropriate objective to help build cyber defence capability across Government and critical infrastructure providers.

20. Optus has a relatively mature security posture and operates a Security Operations Centre which performs security monitoring and detection functions for its networks and customer services. It provides actionable insights on the attack vectors identified, including indicators of compromise.

21. Optus recommends that the benchmark for reporting under the proposed *mandatory incident reporting* regime leverages the definition of 'national cyber incident' included in the Cyber Incident Management Arrangements (CIMA) for Australian Governments.

22. Optus recommends that legislation should be crafted to ensure that the exercise of the intrusive security direction and step-in powers is only available in the most extreme circumstances.

23. Optus recommends that the legislation impose a high decision-making 'hurdle' with suitable checks and balances to ensure the exercise of these intrusive powers is properly justified, and the rights and opinion of critical infrastructure owners is properly considered in any decision.

24. Critical infrastructure providers should be provided with immunity from third-party actions because of steps it has taken in response to a Government security direction or a step-in event in a declared emergency scenario.

BACKGROUND

Optus' position as an Australian telecommunications carrier and carriage service provider

25. The SingTel Optus Pty Ltd group companies in Australia ("**Optus**") serve over 11 million customers each day with a broad range of communications services, including mobile, national, local and international telephony, voice over IP, fixed and mobile broadband, internet access services, subscription and IP television, and content services.

26. To deliver these services, Optus owns and operates fixed, mobile and long-haul transmission and access networks and the largest Australian fleet of satellites. These infrastructure assets provide a set of advanced technology platforms for the delivery of content and carriage services. Optus also has an extensive wholesale business, providing network services to many other carriage service providers.

27. General telecommunications carrier licences have been issued by the ACMA in relation to network units owned and operated by the following Optus group companies:

(i) Optus Networks Pty Limited
(ii) Optus Mobile Pty Ltd
(iii) Optus Vision Pty Limited
(iv) Uecomm Pty Limited
(v) Optus Fixed Infrastructure Pty Ltd
(vi) Uecomm Operations Pty Limited
(vii) Optus Satellite Network Pty Ltd

28. Optus has the following group companies which operate as carriage service providers (as defined is the Telecommunications Act 1997):

(i) Optus Networks Pty Limited
(ii) Optus Mobile Pty Ltd
(iii) Optus ADSL Pty Ltd
(iv) Optus Internet Pty Ltd
(v) Optus Wholesale Pty Ltd
(vi) Uecomm Operations Pty Ltd
(vii) Optus Satellite Pty Ltd
(viii) Virgin Mobile (Australia) Pty Ltd (ceasing CSP operations)

Optus' position as a satellite provider

29. Optus owns and operates Australia's premier satellite fleet, which is used to provide broadcast capabilities for both subscription and free to air television services and a range of other satellite-based services. Optus continues to invest in new satellite infrastructure to expand the technical capability and flexibility of its satellite services, and the capacity they provide to the Australian community for the distribution of content services and other communications services.

Optus' position as a content provider

30. Optus is a national provider of content services to the public in Australia, including services delivered via subscription TV, internet streaming, mobile applications and satellite delivery technology.

31. Optus' content services provide the Australian public with access to a range of premium sports and entertainment content, including Optus Sport (which provides live and on-demand coverage of international football properties such as Premier League, UEFA Champions League and J.League), Apple Music, and the Fetch and Optus TV featuring Foxtel subscription television services.

32. Optus holds subscription television licences under the Broadcasting Services Act for its broadcast of the Optus Sport channels via satellite television and its broadcast of the Optus TV featuring Foxtel service.

Optus' position in the Corporate and Government business market

33. Optus Business is a part of the Singtel Group Enterprise business unit which serves corporate and Government customers in Australia with a range of sophisticated business services – including data services, mobility services and managed ICT services. It has major customers in the finance and government sectors and a range of other major corporate clients. One of the successful and growing pillars of its business model is the provision of a range of innovative and valuable cyber security services

Summary

34. In short, **Optus is the owner and operator of significant national communications infrastructure, and the supplier of important carriage and content services to a large portion of the Australian community. Optus acknowledges the onus this creates to serve its customers and the community with competitive and secure services, and it takes this responsibility seriously.**

35. **Optus sees it as a shared national endeavour between Government and critical infrastructure providers to increase the security and resilience of infrastructure critical to Australia's economic well-being.** Optus recommends that this spirit of shared endeavour should infuse the way the Government's announced policy is enacted through the Parliament, and through the design and implementation of the operational arrangements which form the subsequent steps in bringing life to the policy vision. Several other elements of Australia's Cyber Security Strategy 202 recognise the merits and imperative of a co-operative approach between Government and the private sector.

REGULATORY CONTEXT

36. The communications sector is currently subject to layers of regulation related to the security of networks, infrastructure, carriage services, and the protection of the content of communications and information collected while supplying carriage services. These rules are set out in multiple pieces of legislation including the *Telecommunications Act* (especially Parts 13 and 14), the *Telecommunications (Interception and Access) Act*, the *Crimes Act*, the *Privacy Act* as well as obligations in a range of Industry Codes, Standards and Guidelines.

37. Carriers and carriage service providers already face obligations closely aligned with the stated objectives of the new critical infrastructure regulation. For example, Part 14 of the *Telecommunications Act* (also known as TSSR – the Telecommunications Sector Security Reforms from 2017) sets out detailed rules and processes to support these objectives.

38. The TSSR regime requires carriers and CSPs to do their best to protect telecommunications networks and facilities from unauthorised interference or unauthorised access to ensure:

    (a) the confidentiality of communications; and
    (b) the availability and integrity of telecommunications networks and facilities.

    In practical terms, and as stated in the legislation, TSSR imposes a management duty to maintain competent supervision and effective control over telecommunications networks and facilities owned or operated by the carrier or provider.

39. These TSSR requirements are stated to be for the purpose of security, which is expressed in terms of the protection of the Australian community and the Commonwealth and the States and Territories from espionage, sabotage, attacks on Australia's defence system and acts of foreign interference.

40. The existence of this significant and relevant body of rules should be given significant weight in considerations of how to apply the new critical infrastructure security policy to the communications sector. It is not a green fields scenario.

41. Regulatory best practice principles suggest the next step is to consider how to achieve the policy intent with the least possible regulatory intervention. In the case of the communications sector, this path of least intervention involves making any necessary adjustments to the suite of rules in the *Telecommunications Act*, including TSSR and the other rules regarding the protection of communications.

42. Regulatory best practice principles also suggest new law should be structured to minimise overlap, inconsistency and duplication with existing law. Embedding key aspects of the new policy into the *Telecommunications Act* will ensure that consideration is given to ensuring consistency with existing regulatory structures and reduce the risk of duplication. It would be an associated drafting task to promote consistency between any new policy changes to the *Security of Critical Infrastructure Act* and changes to the *Telecommunications Act.*

43. The *Telecommunications Act* already contains mechanisms which can be used to integrate the new policy into the existing regulatory regime. Apart from those mentioned above this Act also has:

(a) A carrier licencing regime at Part 3; and
(b) Arrangements for extreme circumstances in Part 16: Defence and Disaster Plans.

44. In the past, the carrier licencing regime has been used to impose licence conditions to achieve policy objectives, including regular reporting on the achievement of those objectives. For example, general or specific licence conditions have previously been attached to:

(a) the achievement of infrastructure objectives such as network rollout targets,
(b) community service obligations such as the Integrated Public Number Database; and
(c) competitive and customer objectives such as pre-selection capability and ballots.

45. While the powers in Part 16 are largely untested, the framework it establishes could readily be used to further the new policy objectives.

46. **Optus recommends that the legislative imposition of the new critical infrastructure security policy to the communications sector is primarily via changes to the Telecommunications Act in concert with the proposed new parts of Security of Critical Infrastructure Act.** This approach is consistent with principles of regulatory best practice.

47. Optus recognises the Govt's right to regulate in the national interest and acknowledges the dependency of Australia's economic success on the services and infrastructure provided by key sectors. In enacting its new policy Government should recognise that certain sectors, such as telecommunications, already have relatively mature approaches to security and infrastructure resiliency. The new law should allow calibration to the relative maturity of each sector and leverage existing regulatory regimes to the maximum extent practical.

48. Optus operates in several of the different sectors to which the critical infrastructure laws will apply:

(a) Communications
(b) Data and the cloud
(c) Space

49. Optus' operations in each of these sectors is regulated under the Telecommunications Act either directly or indirectly. As a carrier or carriage service provider Optus' infrastructure and services are regulated directly under the Act, or if not, they are usually supplied to the market or deployed as a bundle with regulated services which has the same practical effect.

50. From a regulatory framework design perspective, it is important to ensure that arbitrary sectoral lines are not drawn which result in differential regulation or standards being applied to entities which leverage common infrastructure, networks or business systems to supply services into different consumer markets. Consistency across sectors should be a clearly articulated objective which guides the development of the new arrangements.

COMMERCIAL CONTEXT

51. Government should give significant weight to the current and prospective commercial environment when calibrating the policy settings for the new critical infrastructure

security legislation and the associated documents and processes which will apply to the communications sector. The commercial viability of the sector is under considerable stress.

52. The communications industry is currently subject to a significant commercial squeeze, because of the impacts of:

(a) The current national economic recession, which has dampened revenue, profitability and growth potential;
(b) The competitive and customer imperative to invest in substantial new technology platforms (e.g. 5G mobile, new satellites, IoT platforms);
(c) The relatively high cost levied by Government for regulated business inputs, such as carrier licences (annual licences fees), contributions to social policy (universal service obligation levies) and spectrum licences;
(d) Disintermediation by 'over the top' providers, which can leverage the network and carriage services provided by network providers at low or no cost;
(e) Successive rounds of national security legislation such as Data Retention, sharing arrangements for the cost of interception, and rules aimed at mitigating the effects of the increasing use of encrypted communications; and
(f) Government decisions and guidance under TSSR, which has fundamentally changed the dynamics of the Australian communications sector, investment climate, supply chain options and the economics of many providers.

53. **The proposed new critical infrastructure security laws are likely to add to the currently high commercial stresses on the communications industry unless Government looks both within the proposed new framework, and also the other policy settings within its control, to moderate adverse impacts on incentives to investment, limit compliance costs and avoid crowding-out legitimate commercial endeavour**.

54. ***Commercial-in-Confidence***

55. ***Commercial-in-Confidence***

Incentives to invest

56. Optus has made annual capital investments of over $1 billion in its infrastructure and associated business operations for at least the last decade. It is currently embarked on significant investment programs in infrastructure including a new 5G stand-alone mobile network, a new satellite, transport network assets and a range of intelligent network capabilities and platforms.

57. The proposed new critical infrastructure law creates a powerful driver of uncertainty over Optus' ability to execute its current investment program as planned. Announcements to date have been at a high level, and the legislation is expected to be at framework level only. It will be some way into 2021 before further detail on possible security standards and key operational aspects is available. It is only then that evaluations of compliance costs can be made, and change requirements identified for in-flight programs.

58. The proposals will also have a chilling effect on the preparation of Optus' capital investment plan for the coming financial year because the real impact of the new security regime is not known and will be difficult to estimate. This plan will be developed for shareholder consideration before the end of calendar 2020, which

parallels the period over which the high-level legislation will be developed and tabled in parliament.

59. Even if Optus could predict with certainty that its current operations will meet the future security standard, provision will still have to be made for substantial expenditure in process development (e.g. incident reporting, sharing of threat information), compliance checking and reporting arrangements (annual reporting on status, reporting of infrastructure assets and ownership) and a substantial program to manage the implementation of all these requirements. This will have the effect of crowding-out other commercially attractive expenditure.

60. Shareholder decisions about Optus' capital plans for 2021 and beyond will have to be made in a climate of uncertainty about the impact of this security regime. While it will be a material factor, it is currently difficult to predict the influence it will have on shareholder decisions about the overall size and focus of Optus' investment program.

61. ***Commercial-in-Confidence***

62. Chart 1: ***Commercial-in-Confidence***

63. Chart 2: ***Commercial-in-Confidence***

64. Chart 3 ***Commercial-in-Confidence***

65. ***Commercial-in-Confidence***

Other considerations – commercial security services

66. Optus' corporate and government business unit, Optus Business, operates a strong security practice offering cyber security and managed security services to protect medium and large enterprise and Government customers against data theft, security breaches, and system failure caused by malware. This is a major commercial pillar and growth engine for the business unit.

67. **Government efforts to build the security posture of critical infrastructure should be designed to work co-operatively, or at least co-exist without damaging commercial enterprise and business solutions aimed at building better security outcomes for Australian businesses.** Government activity promoting security should complement rather than supplant or appropriate the operating space or information necessary to run commercial service offerings.

68. To the extent that the critical infrastructure framework envisages compulsory sharing of threat information, or mandatory reporting of security incidents, these obligations need to be clearly targeted at events relating to a provider's critical infrastructure assets and not at the commercial security services which are offered to customers whose services are typically at the perimeter of the access networks.

CRITICAL INFRASTRUCTURE: DEFINITIONS AND ENTITIES

69. A very broad regulated scope, perhaps too broad, will emerge if the current definition of critical infrastructure is teamed with the proposal to declare the entity which controls the assets as the regulated entity. This approach should be moderated consistent with the principle that regulation should be targeted at the least possible and viable scope to achieve the policy intent.

70. The definition cited in the consultation paper is from the Australian Government's Critical Infrastructure Strategy 2015:

"..those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security."

71. This definition is adequate to convey a high-level descriptive view of the importance of critical infrastructure, but it is too generalised and broad for the purposes of targeting a regulatory regime. A more tightly defined set of definitions should be developed, with specific reference to the nature of critical infrastructure in each regulated sector.

72. The new legislation should include:

(a) high level guidance on the policy intent of the regime aided using the descriptive definition from the Critical Infrastructure Strategy 2015 cited above; and

(b) a mechanism for the subsequent development and declaration of the critical infrastructure elements for each sector, for the separate purposes of defining the practical scope of the new regulatory framework and assisting the identification of the relevant entities to be regulated.

73. In the telecommunications sector the adoption of the term "communications network" as a definition of critical infrastructure would have the effect of capturing within regulated scope a range of infrastructure and assets which if destroyed, damaged or degraded would not have any widespread impact or lead to the consequences outlined in the second half of the description. For example, in a mobile telecommunications network context, a single base station could be destroyed, damaged or degraded without any material impact on the overall operation of the network. The analogous case in the fixed network context is the local loop infrastructure.

74. **The definition of critical infrastructure in a communications network context should focus on the core network elements, those elements which contain the real intelligence of the network and which in practice exercise the command and control functions critical to the proper functioning of the network.** This approach of defining critical infrastructure can accommodate traditional network hierarchies with a central core, and flexibly incorporate newer network technologies which might involve distributing intelligent network nodes away from a central core element.

75. This approach allows for more detailed work to follow the passage of the legislation through Parliament to more fully flesh out the critical network elements and operational support systems ("OSS") which control the availability and integrity of major portions of the various network types (fixed, mobile, satellite, submarine cable etc). This work could be included as a companion piece in the proposed co-design of sector specific security standards.

76. A similar approach can be adopted to targeting the regulated scope as it applies to the business support systems and information technologies employed within carriers and carriage service providers. Many information technology systems operated by carriers and carriage service providers are not relevant or directly related to the critical infrastructure or protected customer information aspects of their operations, and there is no reason for a catch-all definition of critical infrastructure entity and

critical infrastructure to be used which incorporates such systems in the regulated scope.

77. In a communications context, it may be that closer analysis suggests that provisioning systems and certain billing and customer care systems, i.e. the business support systems ('BSS'), operated by carriage service providers are critical to the proper functioning of the critical infrastructure 'ecosystem' and should therefore be included in scope. Such analysis should be carried out as part of the process of co-designing the security standards.

78. In summary, the detailed analysis required for the development of more precise definition for the communications sector should start with (and test) the proposition that critical infrastructure comprises core network elements and the OSS/BSS systems required to support customer fulfilment activities.

79. The specification of regulated entities should leverage existing regulatory definitions to the maximum extent possible. For example, refer to the list of Optus carrier and carriage service provider entities in the background section of this submission. For the communications sector, having the ability to specify entities using these categories provides a well-defined and understood starting point, based on functional activity or ownership of a specified class of assets.

80. **Optus recommends that the task of mapping of potential critical infrastructure entities to the three regulated categories (critical infrastructure provider, regulated critical infrastructure provider and systems of national significance) be delegated by legislation to a subsequent process which has regard to:**

(a) **regulated entity definitions in existing law (e.g. carrier and carriage service provider definitions in the Telecommunications Act);**

(b) **targeted and specific definitions of critical infrastructure developed for each sector (e.g. core network assets of communications networks);**

(c) **technical feasibility and commercial viability of the entity being declared in one or other of the categories; and**

(d) **the principles of simplicity, transparency, accuracy and stability (as referenced in page 14 of the discussion paper), and consistency across sectors to ensure operational effectiveness for entities which happen to operate in multiple sectors.**

81. Optus recommends that the task of mapping of potential critical infrastructure entities to the three regulated categories be informed by specific knowledge gleaned from a consultative process, and that expertise is applied to the task of keeping clear delineation between infrastructure and entity concepts and promoting tight targeting of each. The legislation should require that the process involves:

(a) close consultation with each sector (potential regulated entities and relevant industry associations;

(b) establishment of decision-making processes with clear roles and responsibilities (for the Minister, Department of Home Affairs, sector technical experts, industry associations and potential regulated entities);

(c) suitable procedural fairness, for example, exposing of preliminary views and instruments, rights for proposed regulated entities to provide further information or evidence, and an appeal process.

82. **Optus recommends that the scope of regulation be defined by the cross section of an entity definition and asset definition:**

(a) **The regulated entity - which owns and operates defined critical infrastructure assets;**

(b) **The defined critical infrastructure (e.g. core network assets) owned by the regulated entity; and**

(c) **Excluding business activities and assets which are not directly related to the critical infrastructure assets or activities.**

83. Optus acknowledges the list of sectors which Government intends to include in the regulatory construct:

- Banking and finance
- Communications
- Data and the Cloud
- Defence industry
- Education, research and innovation
- Energy
- Food and grocery
- Health
- Space
- Transport
- Water

84. Optus recommends consideration be given to ensure the list of sectors covers directly, or indirectly, the following:

- 'Over the Top' service or application providers
- Critical data centres
- Internet route and domain registries
- Satellite and terrestrial communications
- Submarine communications cable operators

85. It is important to include 'over the top' application providers into the scope of this new security regime because through their operations and applications, these companies extract and hold significant quantities of data about the Australian community, it habits, movements, purchasing preferences and other personal information. If this data was currently held by a carrier or carriage service provider, it would be protected by the provisions of Part 13 of the *Telecommunications Act*. In future, it would likely also be protected in the hands of a carrier by the new security regime. Comparable protections should be afforded to uses of OTT services via the application of the new regime to that sector.

POSITIVE SECURITY OBLIGATION

86. The consultation paper outlines that a positive security obligation with reference to the high level, sector-agnostic principles that will form the basis for the legally enforceable oblations. The paper suggests the following principles:

(a) ***Identify and understand risks*****:** entities will have a responsibility to take an all-hazards approach when identifying and understanding risks.

(b) ***Mitigate risks to prevent incidents*****:** entities will be required to have appropriate risk mitigations in place to manage identified risks applicable to their sector

(c) ***Minimise the impact of realised incidents*****:** entities will be required to have robust procedures in place to recover as quickly as possible in the event a threat has been realised

(d) ***Effective governance*****:** entities will be required to have appropriate risk management oversight and responsibilities in place, including evaluation and testing.

87. **Optus acknowledges these high-level principles form a suitable generic framework of for the development of the Positive Security Obligation and guiding risk management and governance arrangements for regulated entities**. The principles are appropriately high level and leave suitable flexibility for operational arrangements to be calibrated to reflect the scenarios arising in a sector, entity, technology type or supply chain arrangement.

88. The consultation paper says the new framework will clearly set out in legislation the high-level security obligations that critical infrastructure entities should meet:

(a) ***Physical security*****:** critical infrastructure entities will be required to protect their systems and networks by considering and mitigating natural, and human induced threats

(b) ***Cyber security*****:** critical infrastructure entities will protect their systems and information from cyber threats. This may include:

(c) ***Personnel security*****:** critical infrastructure entities will implement policies and procedures which seek to mitigate the risk of employees (insider threats) exploiting their legitimate access to an organisation's assets for unauthorised purposes.

(d) ***Supply chain security*****:** Critical infrastructure entities will protect their operations by understanding supply chain risk.

89. Optus acknowledges that these high-level obligations create a suitable generic framework to guide the development of the Positive Security Obligation and more detailed sector-specific security standards. Optus currently has regard to the "all hazards" approach articulated by these four aspects of security analysis and governance.

Co-design of security standards

90. **The proposed new security standards should adopt a risk-based approach**, which requires the identification of specific risks to be managed and then provides flexibility for critical infrastructure providers to select or design controls based on their specific network architecture, technology choices, vendor mix and operational context. The standards should not be overly prescriptive in terms of mandating specific technology solutions which may reside in some or only one vendor's equipment but not in others.

91. It is critical that regulated entities have a seat at the table for the process which selects or develops the security standards. This is important to promote procedural fairness and to ensure to that industry considerations, experience and capability informs the both the process and the outcome.

92. **The legislation should be structured to ensure the process of declaring or determining the applicable industry standards should have suitable checks**

and balances, for example, the decision-maker should be compelled to have regard to:

(a) Technical feasibility, and the availability of the means to comply with requirements;
(b) Commercial viability, the legitimate commercial interests of the entities in the sector;
(c) Proportionality, does not impose an undue cost burden
(d) Effectiveness and efficiency
(e) Consistency with standards in other sectors
(f) Global precedents or security 'best practice' norms

93. Given that a number of critical infrastructure providers have operations in more than one of the regulated sectors, it will be important from an efficiency and cost management perspective for the standards applicable to each of the adjacent sectors to be aligned and operate consistently. It will reduce the overall efficiency of the ecosystem and detract from the achievement of desired policy outcomes if the same (or similar) infrastructure is held to different security standards by different industry regulators because the infrastructure is used to generate services in more than one regulated sector.

Cost analysis and implications

94. **Optus recommends that the Department of Home Affairs accept that the information released to date does not provide a reasonable basis for entities or sectors to contribute quantitative information to a cost-benefit analysis or regulatory impact assessment of the proposed framework.** Any quantitative cost or impact estimates produced at this stage will be inherently unreliable.

95. Cost and impact analysis is a detailed task which is reliant on the ability to perform (at least) a comparison and gap analysis between current state and the specific requirements of the future state. The steps required to address the identified gaps can then be scoped, designed, costed and an implementation schedule estimated.

96. **Commercial-in-Confidence**

97. **Commercial-in-Confidence**

98. **Commercial-in-Confidence**

99. ***Commercial -in-Confidence***

100. **Optus considers that vital details of the future state of the positive security obligation are not yet available and hence a quantitative cost analysis cannot be undertaken.** For example, the regulated security standards are not known, and process architecture for mandatory information sharing and incident reporting is not described. Additional definitional information necessary for such an analysis is also not yet available, including a confirmed definition of 'critical infrastructure', 'system of national significance' and 'regulated entity', each of which is subject matter in this consultation.

101. The prospect of an entirely new regulatory regime being imposed into the operating environment of a commercial entity is a material development. Any new environment, even the most 'light touch', will necessitate adjustments to existing arrangements to manage new obligations and risks, to deal with new or expanded

regulators, to moderate commercial plans or in-flight programs and to ensure suitable governance frameworks are in place and functioning effectively.

102. **Optus anticipates that compliance arrangements triggered by the proposed new regulatory obligations will have cost, employment and process impacts, in both the short and the long term, across all major categories of corporate activity involved in managing its carrier and carriage service provider business operations**, including:

(a) Governance and risk - reporting assessment and management, up to Board level
(b) Management, operational and commercial
    (i) Budgeting and financial planning
    (ii) Reporting and monitoring
    (iii) Updates to corporate policies
    (iv) Corporate risk assessment
    (v) Rate of return on investment, and forgone investment opportunities
    (vi) Project resourcing and management
    (vii) Structure of asset registers
    (viii) Impacts on commercial security services
(c) Technical design and architecture (network and IT)
    (i) Network topology and segregation
    (ii) Deployment processes - physical and logical
    (iii) Speed of replacement or upgrade of assets
    (iv) Scope of local, regional and global operations
    (v) New strategic partnerships
(d) Procurement processes
    (i) Tenders
    (ii) Balance of insourcing versus outsourcing
    (iii) Legal contracting, liability and indemnity
    (iv) Vendor selection
    (v) Vendor support arrangements
(e) Security administration
    (i) Reviews of control environment
    (ii) Potential new common control infrastructure
    (iii) Control monitoring
    (iv) Control reporting and evaluation
    (v) Physical security
    (vi) Incident investigation processes and reporting
    (vii) Processes to share threat information
    (viii) Information sharing processes
    (ix) Development of security event playbooks
    (x) Participation in playbook rehearsals
    (xi) Data and log storage and analysis capabilities
    (xii) Potential use of artificial intelligence and machine learning
    (xiii) User behaviour and anomaly monitoring
    (xiv) Threat Intelligence and management
(f) Personnel management
    (i) Employment levels and expertise
    (ii) Recruitment policies and practices
    (iii) Government and regulator liaison staff
(g) Regulatory overhead
    (i) Regulatory reporting

(ii) Independent audit costs
(iii) Planning for potential Government step-in scenarios
(iv) New record keeping requirements
(v) Responding to security notices from the regulator
(vi) Responding to regulator investigations and requests for information

This is an illustrative list complied on a non-exhaustive basis to demonstrate the scope of the task which will be faced by regulated entities to assess potential cost impacts. Other functions and processes are also likely to be affected.

Implementation periods

103. Critical components of the regulatory framework which set out the operational details and obligations are slated for development in 2021 after the passage of the legislation. These include:

(a) The co-design of sector specific security standards
(b) The various information sharing and reporting processes
(c) Incident reporting processes and criteria
(d) Precise definitions of regulated entities and infrastructure

104. Until these design tasks are completed it will not be possible for regulated entities to predict with any precision the time period required to achieve compliance. This makes it critical for the new legislation to accommodate reasonable implementation and transition periods.

105. **Optus recommends the proposed legislative framework provides adequate time for designing and implementing key components**, including:

(a) The development and specification of obligations and processes not already fully described in the legislation (e.g. sector specific security standards);
(b) The evaluation by regulated entities of current practice against the new operational requirements;
(c) A process for evaluating the time needed to implement the various components; and
(d) A decision-making process for determining reasonable implementation periods to achieve compliance.

This important work should not be compromised by artificially tight deadlines.

COMMUNICATIONS INDUSTRY SECURITY REGULATOR

106. The Telecommunications Sector Unit within the Critical Infrastructure Centre in the Department of Home Affairs is effectively assigned a regulatory role over the communications sector by Part 14 of the *Telecommunications Act* (the TSSR provisions). In exercising responsibilities under the TSSR regime over recent years it has built up a body of expertise and knowledge which cannot easily be replaced or replicated.

107. The consultation paper outlines an expectation that the sector regulators will enforce the positive security obligation requirements through flexible administrative measures and graduated enforcement powers. Compliance and enforcement action (in line with

the *Regulatory Powers Act 2014*) is described in page 23 of the consultation paper to include:

(a) overseeing compliance with the legislative obligations (other compliance powers, evidenced through reporting to the regulator and timely responses to security notices);
(b) the ability to issue requests for access to information, and inspection and audit powers;
(c) issuing security notices that entities would need to consider and evidence in their reporting as part of meeting their obligations;
(d) provide detailed guidance on how to achieve compliance;
(e) the ability to intervene and issue directions in cases where there are significant national security concerns that cannot be addressed through other means; and
(f) the ability to issue penalties for non-compliance.

108. **Optus considers it reasonable for the Telecommunications Sector unit of the Critical Infrastructure Centre to be assigned the role as regulator of the communication sector under the new framework**. This would allow the benefits of continuity, expertise and experience from the current TSSR regime to be bought forward into the new regime.

109. **Optus considers it important for legislation to set out the regulatory policy intent that the new security law be administered by regulators which function co-operatively with regulated entities, i.e. they have a mandate to operate with a 'light touch' regulatory ethos**. A collaborative approach is most likely to yield positive outcomes and further the objectives of the regime, including open information sharing and building baseline capability. This is especially relevant to the implementation of the stated objective that the regulator will provide detailed guidance on how to achieve compliance.

110. The process to develop sector-specific security standards will be enhanced if the new regulators have a clear legislative mandate to work co-operatively with entities within their jurisdiction. There should also be guidance for regulators encouraging them to manage the role of monitoring and enforcing standards in a collaborative and light-touch manner, seeking to foster improved outcomes rather than search for opportunities to impose punitive penalties.

111. The guidance for regulators should also cover proposed regulatory methodology, including the need for:

(a) Discussion with industry sectors, industry associations and entities about best practice
(b) Ensuring obligations are understood
(c) Maintaining two-way discussions to build understanding
(d) Collaborative work to promote best practice security culture

TWO-WAY AND MANDATORY INFORMATION FLOWS

112. The consultation paper envisages a regulatory ecosystem which fosters a range of information flows between regulators and regulated entities, including:

(a) An *annual reporting obligation* on regulated entities to provide information on risk and risk management to their sector regulator. Such reporting would involve

Board level engagement. The proposed reporting would articulate the risk identification mechanisms, risk mitigations activities and outline accountability. Reporting would also address any issues identified for action by the regulator or security incidents that have occurred in the preceding year and actions taken to address those incidents;

(b) Reporting of *threat information in near real time*, including intelligence insights and trends (initially voluntary, and likely moving to a mandatory phase for systems of national significance). It is understood that this will be a two-way process with entities contributing to the development of a national threat picture, and in turn, receiving information back which will assist their management of threats to their critical infrastructure;

(c) Mandatory *incident reporting* of cyber events experienced by regulated entities to the Australian Cyber Security Centre;

(d) Information to support the development of so-called 'play-books' for cyber events and crisis situations; and

(e) Directions or security notices requiring or advising entities to do certain things.

Potential regulatory burden

113. **Optus is concerned that the overall net effect of this series of proposed new information exchange processes could impose undue bureaucratic burden (cost and process) on regulated entities.** To mitigate this risk, Optus requests that the detailed objectives of any reporting and information exchange protocols are solidly tested and agreed between entities and regulators, and that the efficiency and effectiveness of proposed methods and processes is validated before being mandated or implemented.

Threat intelligence platform and sharing threat information

114. **Optus supports the policy vision that improved situational awareness, including the development of a near real-time national threat picture, is an appropriate objective to help build cyber defence capability across Government and critical infrastructure providers.** The challenge is to do this in an efficient and effective way.

115. A suitable next step is for Government or the ACSC to outline plans, draft interface specifications, data formats etc and consult with industry on scoping of a Threat Intelligence Platform to service the proposed information sharing process. This is an architectural and design task, not a policy one, and so the best approach is to get the technologists working on it as soon as is reasonably practical. Once specifications are determined then proposals for budget and implementation activities can be developed and agreed.

116. The threat sharing process should be designed to operate using end-to-end automation, or automation to the maximum extent possible. This is to ensure operational costs are limited and activity can be contemporaneous. Secure engagement channels will also be required to discuss and share analysis of events and situations. Government must tackle and develop solutions to the challenge of making otherwise classified threat information available in actionable form to critical infrastructure providers.

117. Some sectors and entities are more mature than others in their capability to monitor and detect threats, and the more sophisticated providers can be on-boarded to the threat sharing arrangements sooner with others following as capability expands. Optus operates a Security Operations Centre which performs security monitoring and detection functions for its networks and customer services. It provides actionable insights on some of the attack vectors identified, including indicators of compromise.

118. Optus also uses the following techniques to identify vulnerabilities at the perimeter of its networks (a non-exhaustive list) and inform its security status:

(a) Netflow based Telemetry
(b) DDoS Mitigation Systems
(c) Firewalls and IPS Alerts
(d) SIEM analysis of events
(e) Monitoring logs of authentication systems
(f) Vendor notifications
(g) Vulnerability scanning and penetration testing

Incident reporting

119. **Optus recommends that the benchmark for reporting under the proposed *mandatory incident reporting* regime leverages the definition of 'national cyber incident' included in the Cyber Incident Management Arrangements (CIMA) for Australian Governments**. These Arrangements define a national cyber incident as a cyber incident that:

(a) significantly impacts, or has the potential to significantly impact, multiple Australian jurisdictions, and/or
(b) requires a coordinated inter-jurisdictional response.

120. The CIMA documentation sets out that a national cyber incident could affect multiple jurisdictions simultaneously or could pose a threat to multiple jurisdictions after initially affecting a single jurisdiction. Examples of potential national cyber incidents include:

(a) an organisation with links across multiple jurisdictions being compromised through a cyber incident
(b) malicious cyber activity affecting critical national infrastructure where the consequences have the potential to cause sustained disruption of essential services or threaten national security
(c) malicious cyber activity where the cause and potential extent of its geographic impact is uncertain
(d) a large-scale information system breach of sensitive data affecting persons or organisations in multiple jurisdictions

Playbooks

121. Optus would be pleased to work co-operatively with relevant Government agencies and other communications companies and industry associations (such as Communications Alliance) to develop playbooks on how to respond and manage common sector specific threats. Enabling a broad set of regulated entities to contribute to playbooks will promote standardised approaches across the sector.

122. Playbooks should be developed having reference to industry best practice methodology, for example, the MITRE framework. The logic embedded within a well written playbook will overcome vendor-specific implementation issues because the

guidance can be consumed by different vendor platforms. Playbooks should include at a minimum:

(a) Indicators of Compromises (Hashes, filenames, IP addresses, signatures etc)
(b) Techniques of exploitation
(c) Tools used
(d) Processed used

Directions and emergency step-in powers

123. The regime described in the consultation paper envisages granting two intrusive powers to Government:

(a) The power to issues directions in response to an imminent cyber threat or incident; and
(b) Step-in powers enabling Government to take direct action in the case of declared emergency situations.

124. **Optus recommends that legislation should be crafted to ensure that the exercise of these intrusive direction and step-in powers is only available in the most extreme scenarios.** This is because critical infrastructure providers will typically be in the best position to protect and understand how to defend their infrastructure from attack and they should be able enjoy the benefits of ownership rights over their assets without external interference.

125. **Optus recommends that the legislation impose a high decision-making 'hurdle' with suitable checks and balances to ensure the exercise of these intrusive powers is properly justified, and the rights and opinion of critical infrastructure owners is properly considered in any decision**. There should be a hierarchy of potential actions with priority given to voluntary and cooperative responses before intrusive powers can be triggered.

126. There will always be a risk that the incorrect exercise of coercive powers could have drastic and unforeseen consequences on the infrastructure which the orders were intended to protect, so every effort should be made to involve and leverage the expertise of the infrastructure owner before direct action is taken.

127. **Critical infrastructure providers should be provided with immunity from third-party actions which may arise from adverse outcomes resulting from the provider acting in response to a Government direction or a step-in event**.

128. Apart from the above high level comments and cautions above, it is difficult for respondents to articulate a more fully detailed response because the consultation paper does not put forward a specific model for how these powers will be structured, who will exercise the decision making and how the governance and oversight model will function.

129. **Optus recommends the Government provides an exposure draft of the legislation to prospective regulated sectors and entities so they can comment on a specific model of how these intrusive powers might work and how decision-making criteria might be structured.** This will be an important step to ensure critical infrastructure providers have a voice and an early opportunity to evaluate the details of the high-level proposal described in the consultation paper.

End.