PROTECTING AUSTRALIA'S CRITICAL INFRASTRUCTURE AND ESSENTIAL SERVICES SBS RESPONSE TO CONSULTATION PAPER

SEPTEMBER 2020

Introduction

The Special Broadcasting Service Corporation (**SBS**) appreciates the opportunity to comment on the Department of Home Affairs *Protecting Critical Infrastructure and Systems of National Significance – Consultation Paper* (the **Consultation Paper**). SBS supports the Government's focus on critical infrastructure and essential services, and the mitigation of risks associated with them.

As Australia's only nationally available multilingual and multicultural broadcaster, it is the principal function of SBS to provide radio, television and digital media services that inform, educate and entertain all Australians and, in doing so, reflect Australia's multicultural society.[1]

SBS reaches almost 100 per cent of the population through its six free-to-air TV channels (SBS SD, SBS HD, SBS VICELAND HD, SBS World Movies, SBS Food and National Indigenous Television (NITV)) and seven radio stations (SBS Radio 1, 2 and 3, SBS Arabic24, SBS PopDesi, SBS Chill and SBS PopAsia). Servicing 63 languages including SBS Arabic24, SBS Radio is dedicated to the nearly five million Australians who speak a language other than English at home, while the three music channels (SBS PopAsia, SBS PopDesi and SBS Chill) engage all Australians through music and pop culture from around the world.

SBS's reach is being significantly extended through SBS's digital services, including SBS On Demand, the SBS Radio App and portals which make online audio programming and information available to audiences at a time and place of their choosing.

SBS provides its services in partnership with a range of private entities who own the infrastructure that is uses to distribute SBS content.

Proposed coverage of the framework

As set out in the Consultation Paper, it is appropriate that the proposed framework:

- provide proportionate requirements developed in consultation with industry;
- acknowledge that one size does not fit all when it comes to safeguards; and
- takes a principles-based approach.

SBS will continue to engage constructively with the framework development process, including mapping and identifying which entities should be classified a 'critical infrastructure entity' and 'regulated critical infrastructure entity', taking these principles into account.

[1] SBS Charter.

Noting the intention to apply the framework to owners and operators of relevant critical infrastructure, the most efficient way to safeguard SBS's services—especially with the respect to the broadcast of essential information during emergencies—is to focus on the infrastructure required for the ongoing provision of SBS services, including transmission, telecommunications, cloud and data storage and utilities services provided to SBS.

Based on the descriptions set out in the Consultation Paper, SBS would therefore most appropriately be classified as a 'Critical Infrastructure Entity' under the framework and remain eligible for Government Assistance. SBS would not, however, be required to implement the Positive Security Obligation, or the Enhanced Cyber Security Obligations that would apply to entities in the 'Regulated Critical Infrastructure', 'Systems of National Significance' or 'Whole of Economy' categories.

Implementation of the framework

The Consultation Paper notes that the Positive Security Obligation will have '…set and enforced baseline protections against all hazards for critical infrastructure and systems, implemented through sector-specific standards proportionate to risk'.[2] Should the Positive Security Obligation be applied to entities that own infrastructure used to supply SBS's services, consultation should be undertaken on these sector-specific plans to ensure that they increase security, without enforcing a disproportionate cost and operational overhead on organisations and businesses with which SBS partners. Appropriate safeguards would also need to be in place to ensure the security of any information provided by SBS or its partners under this framework.

While not captured by all aspects of the framework, SBS would be pleased to participate in the sector-specific consultations to support its infrastructure partners in the development and implementation of the framework. As noted above, a principles-based outcome would be preferred over a prescriptive requirement, to recognise the significant investment that SBS's infrastructure partners already make in physical and cyber security.

Through the sector-specific consultation the following issues should be considered.

Regulation of the Positive Security Obligation

The broadcasting sector is heavily regulated in relation to its operations, with the Australian Communications and Media Authority (**ACMA**) undertaking many of these responsibilities. Care should be taken to ensure that duplication with existing internal and external reporting, risk assessments and internal audits is minimised.

The introduction of the Positive Security Obligation should also be considered in relation to existing interactions with the Australian Signals Directorate (**ASD**) and the Australian Cyber Security Centre (**ACSC**).

There may be opportunities for critical communications infrastructure operators to work together to provide reporting under the Positive Security Obligation, therefore reducing the impact on individual organisations and businesses. This would also ensure a standard industry procedure for the implementation and reporting of the Positive Security Obligation.

[2] Consultation Paper, page 10

Existing security measures

SBS is critically dependent on the supply chains of utility providers and their infrastructure (e.g. ERM Power, Ausgrid and Sydney Water). We note that these utilities are captured in the existing critical infrastructure security framework, and their obligations may be expanded.

BAI Communications, which manages SBS's transmission facilities, has a mature operational regime in place for protecting the resilience of infrastructure under extreme conditions, as well as pragmatic protection from intruders. Following the 2019-20 bushfires, BAI has been developing its capabilities in concert with other infrastructure operators and emergency services.

Telstra, Optus, and NBN Co are also key service providers to SBS, as well as Akamai and Amazon Web Services. These companies have highly resilient infrastructure and contingency capabilities to address major network failures.

Enhanced Cyber Security Obligations

SBS operations rely on the security of data transfer and storage. Cyber security is therefore vital to SBS's continuing operations and has been a key focus in recent years. While SBS would not be captured by the Enhanced Cyber Security Obligations under this framework, any assistance from the Government with respect to enhancing SBS's cyber security capability would be of benefit.

These preparatory activities, depending on their scope, may impact SBS with respect to resourcing and cost of mitigating any identified vulnerabilities. Similarly, there may be overlaps with existing cyber security initiatives. Participation in these should be optional.

A mandatory notification threshold could be established to develop a near-real time aggregated threat picture. This would increase the speed at which information can be made available to organisations and businesses about a recent cyber security incident and improve these organisations' ability to protect themselves from a similar breach. The ACSC does provide this information when available, however, organisations and businesses are not obligated to report successful cyber-attacks.

Threat intelligence technology providers should also be involved, as they provide early warning signs of imminent threats.

The Consultation Paper recommends the introduction of a 'Playbook' which would include '…response plans for a range of scenarios'[3]. While this should be shared with key organisations and businesses, the secure storage of the information set out in the Playbook should be considered to ensure that it cannot be accessed or circumvented by threat actors.

Government Assistance

The Consultation Paper notes that '[i]t is anticipated that the Government assistance element of the framework will be primarily discharged on a voluntary basis, as entities will also want to restore functions expeditiously… Government needs to have a clear and unambiguous legal basis on which to act in the national interest and maintain continuity of any dependent essential

[3] Consultation Paper, page 27

services.'[4] The current National Terrorism Threat Advisory System may provide guidance for this to the extent that the National Security Division would be the most appropriate security agency to determine a response to protect Critical Infrastructure.

[4] Consultation Paper, page 29