16 September 2020

Systems Engineering Society of Australia
PO Box 3892
Manuka ACT 2603

RE Australian Government Consultation Paper on:
"*Protecting Critical Infrastructure and Systems of National Significance*"

To whom it may concern,

The Systems Engineering Society of Australia (SESA) is the Australian chapter of the International Council on Systems Engineering (INCOSE) and a technical society of Engineers Australia. SESA has cross-domain and sector membership focused on bridging the specialisations through the transdisciplinary application of systems principles and concepts in the efficient and effective engineering of systems for a better, safer world.

SESA represents over 700 systems experts around Australia from Government, Industry and Academia across Defence, Aerospace, Transport, Infrastructure, Education, Telecommunications, Smart-Cities, Automotive, Healthcare and Energy. SESA is the only systems-thinking focused society in Engineers Australia, contributing to international standards and the Systems Engineering Body of Knowledge (SEBOK).

SESA's feedback to the Australian Government's consultation paper on "*Protecting Critical Infrastructure and Systems of National Significance*" is provided in two parts:

1. General feedback on the scope and approach of the consultation paper; and
2. Specific feedback related to questions noted in the consultation paper.

The SESA Resilience Working Group would be pleased to discuss the contents of this response in more detail with Government in the next steps of their consultation process.

[redacted]
Jawahar Bhalla (Technical Director of SESA)
e-mail: [redacted]

SESA Resilience Working Group [Jawahar Bhalla (JB Engineering Systems), Thomas Manley (Downer), Grace Kennedy (University of Wollongong), Kevin Robinson (Shoal), and Chris Browne (Australian National University)]

[Part 1: General Feedback]

SESA notes and commends the recognition of systems concepts in the consultation paper, such as the increasing interconnectedness and interdependence of Critical Infrastructure (CI) Systems and the risk of unintended consequences that may result and the vulnerabilities that these could create (pages 4, 6, 8). The Government has indeed gone to great lengths to include inputs from across sectors and industry. The prime focus of this SESA submission is to build on and complement the excellent foundational work in the consultation paper from a systems-thinking and "whole of life" perspectives.

The following are general comments from SESA's review of the consultation paper in terms of SESA observations and SESA recommendations, for Government consideration and subsequent discussion:

1. Terminology and Language - "Security and Resilience"

1.1. **SESA Observations**[1]

1.1.1. The stated primary objective of the proposed enhanced framework in the consultation paper is to *"protect Australia's critical infrastructure from all hazards*" (page 9) with the intent to initiate a "*refreshed Critical Infrastructure Resilience Strategy*" (page 4), yet the framework described appears to focus solely on security (to the exclusion of resilience). Resilience appears to be "added on" as an associated but separate aspect ("security and resilience" used in various instances).

1.1.2. SESA notes that a large part of (cyber) security [the ability to deal with (cyber) threats to security] forms part of resilience, and that resilience is a "larger concept" encompassing numerous other dimensions, and therefore is of relevance to the paper. However, the approach to the usage of these two concepts, and the lack of an ontological definition, detracts from the clarity and intent of the paper. The initiatives given only cover cybersecurity, not resiliency.

1.1.3. The use of "security and resilience" suggests two separate concepts, whereas they are inherently linked. Clarity could be improved through better contextualisation and definitions of these central concepts.

1.1.4. If the framework is broader than security, then consider including obligations related to resilience of CI Capability Systems such as:

a) Reliability and availability targets;
b) The requirement to conduct (and report on) regular resilience assessments;
c) The requirement to perform (and report on) regular disaster recovery testing (including through modelling and simulations were appropriate); and
d) The requirement to mitigate all identified Single Points of Failure (SPOF) and ensure adequate levels of physical (and functional) redundancy exist.

1.2. **SESA Recommendation** - The Government should establish a common definition for resilience in an Australian context that could then be tailored and applied consistently across sectors and domains providing for alignment of understanding and integration of approaches.

[1] Consultation Paper Reference Pages 4, 9, 12, 15, 19.

2. A Focus on the Physical Elements of Systems

2.1. **SESA Observations**[2]

2.1.1. The language used through the paper suggests an implicit (and at times explicit) focus on physical aspects of systems, or on tangible (technological) elements of systems.

2.1.2. A "System" is more than just the physical components (technological/hardware/software) that form its tangible parts, it is the synthesis of the holistic system that enables the understanding of critical capability or essential services that will be of relevance in the development of the enhanced framework being proposed.

2.1.3. A System includes the people (capacity, competency), processes, tools, technical data, resources and enabling support systems and services across applicable whole-of-life use-cases. In fact it is *the essential enabling relationships* (systems and services) associated with a Critical Infrastructure system that is key to its resilience (and security), and these are where the focus of such initiatives need to be directed (over the tangible components that male up the critical capabilities).

2.2. **SESA Recommendation** – The Government should apply a holistic systems view of Critical Infrastructure ensuring identification of all associated critical elements that comprise the Critical Infrastructure System and its associated essential enabling interfaces/relationships so as to minimise the risk of unintended consequences that may result in the loss of critical capabilities in threat situations.

3. A Focus on Fielded Systems and "Owners & Operators"

3.1. **SESA Observations**[3]

3.1.1. The terminology used in the consultation paper, such as the specific reference to "Owners and Operators" suggests an implicit focus on fielded systems, and specifically on the operational use of these systems.

3.1.2. This theme is reflected in the three-part "features of the enhanced framework" (page 10) focused on the "protections" to be built / added to systems that are in use/operation (i.e. fielded).

3.1.3. The consultation paper is silent on aspects such as maintenance and modification of fielded Critical Infrastructure systems (or suggests / assumes these are within the mandate of "owners and operators"), and equally if not more importantly, on the engineering (definition, realisation, delivery into service and subsequent modifications) of future Critical Infrastructure systems.

3.1.4. A "whole-of-life" perspective will ensure maximum scope coverage (and risk mitigation) in the context of security and resilience.

3.1.5. Consideration must be given to both the protection of fielded systems that are in operational use as well as to the definition (design right) and realisation (build right) of new systems, and to the maintenance and modification of fielded systems (to ensure ongoing integrity of design).

3.1.6. This could potentially be factored in as fourth part (focused on engineering CI systems to build-in security/resilience and on ensuring retention of design integrity through

[2] Consultation Paper Reference Pages 8, 11, 13.

[3] Consultation Paper Reference Pages 4, 8, 9, 10, 12, 13, 14, 22, 25, 26.

modifications and maintenance) to the three-part "enhanced framework" approach proposed in the consultation paper at page 10 towards a whole-of-life view

3.2. **SESA Recommendation** – The Government consider refining the proposed "enhanced framework" to consider a whole-of-life perspective that considers not just use/operation of Critical Infrastructure systems but also their definition, realisation, maintenance and modification – especially relevant in our present environmental context of ever increasing rates of technological change and obsolescence.

4. Classes of Entities and Relevant Elements of the Framework

4.1. **SESA Observations**[4]

4.1.1. The consultation paper implies that the Critical Infrastructure sectors will expand from the previous nine sectors (inclusive of Space) to include Data and the Cloud; and Education, Research and Innovation; with a shift from Commonwealth Government to Defence industry.

4.1.2. These Critical Infrastructure Sectors are also identified in the consultation paper as Critical Infrastructure *Entities*. A subset of these Critical Infrastructure *Entities* are referred to as Regulated Critical Infrastructure Entities (presumably equivalent to the Critical Infrastructure *Assets* identified in the *Security of Critical Infrastructure Act 2018*). Further subsets are *Systems of National Significance*. This creates a hierarchy of criticality with four distinct levels:

a) Whole of Economy (least critical)
b) CI Entities (previously CI Sectors)
c) Regulated CI Entities (previously CI Assets)
d) Systems of National Significance (most critical).

4.1.3. The re-use and duplication of terminology may be confusing to those seeking to understand the framework.

4.1.4. Additionally, the term 'entities' appears to imply the identification of organisations rather than capability systems that they help to provide.

4.1.5. Note that many systems do not have a single identifiable owner e.g. Australian Tsunami Warning System (ATWS) that is jointly delivered by Geoscience Australia, the Bureau of Meteorology (BOM) and the Crisis Communications Centre (CCC) within DHA. Similarly, the electricity network is a combination of elements provided by generators, distributors and retailers as opposed to a single entity.

4.2. **SESA Recommendation** – The Government consider refining concepts and terminology to improve clarity of context and scope of CI artefacts covered by the framework, such as focusing on capability of systems (inclusive of socio-technical elements) instead of organisations (entities) and the establishment of a register of CI capability systems (covering CI Assets and Systems of National Significance along with identification of system boundaries and their essential enabling relationships) so there is no ambiguity as to what CI

[4] Consultation Paper Reference Pages 3, 11.

[Part 2: Specific Feedback]

Refer to table below for specific SESA feedback against the questions in this consultation paper.

Question #	Consultation Paper Question & SESA Response
1	*Question: Do the sectors above capture the functions that are vital to Australia's economy, security and sovereignty? Are there any other sectors that you think should be considered as part of these reforms (e.g. manufacturing)?*
	Response: The list of critical sectors appears to have been expanded to include Data & the Cloud, Defence Industry and Education, Research and Innovation. Types of infrastructure that do not easily fall into a sector include: • Emergency Response Infrastructure such as police, ambulance and fire-fighting bodies including volunteer bodies such as the State Emergency Services and state-based volunteer bushfire fighting bodies as well as safety systems such as those that support emergency locator beacons; • Defensive Infrastructure that helps to mitigate disasters (such as storm water systems that protect against flood events, or biosecurity controls such as sentinel bee hives that prevent the importation of pests and diseases e.g. varroa mite); and • Situational Awareness Infrastructure that monitors environmental systems and helps provide early warning of potential disasters (including those systems related to the monitoring or weather, air quality, earthquakes, tsunamis, fire and flood etc). The following functions/sectors should also be considered: • Manufacturing and supply chains are essential to underpin all critical infrastructure; • Raw resource/commodities management (this is a large sector for Australia, and pertinent to sovereign capability); • Dams, Chemical, Nuclear, Commercial facilities and Government facilities are additional sectors from the US and UK Critical National Infrastructure Lists; It will be important to not only consider the protection of infrastructure that is required to maintain capability, but also to be aware of those systems that are a potential danger to the public under adverse conditions (e.g. nuclear, chemical, hazardous waste). Note that there is not a one to one mapping between vital functions and sectors. A different approach might be to identify the vital functions first, and then determine what contribution to those functions is made by each sector and/or system. Refer also to SESAs general comment #1 (Terminology and Language - "Security and Resilience"), #2 (A Focus on the Physical Elements of Systems), #3 (A Focus on Fielded Systems and "Owners & Operators") and #4 (Classes of Entities and Relevant Elements of the Framework). Types of infrastructure that do not easily fall into a sector include: • Emergency Response Infrastructure such as police, ambulance and fire • Defensive Infrastructure that helps to mitigate disasters (such as storm water systems that protect against flood events, or biosecurity controls such as sentinel bee hives that prevent the importation of pests and disease • Situational Awareness Infrastructure that monitors environmental systems and helps provide early warning of potential disasters (including those systems related to the monitoring or weather, air quality, earthquakes, tsunamis, fire and flood etc).

	The following functions/sectors should also be considered: • Manufacturing and supply chains are essential to underpin all critical infrastructure; • Raw resource/commodities management (this is a large sector for Australia, and pertinent to sovereign capability); • Dams, Chemical, Nuclear, Commercial facilities and Government facilities are additional sectors from the US and UK Critical National Infrastructure Lists; It will be important to not only consider the protection of infrastructure that is required to maintain capability, but also to be aware of those systems that are a potential danger to the public under adverse conditions (e.g. nuclear, chemical, hazardous waste). Note that there is not a one to one mapping between vital functions and sectors. A different approach might be to identify the vital functions first, and then determine what contribution to those functions is made by each sector and/or system. Refer also to SESAs general comment #1 (Terminology and Language - "Security and Resilience"), #2 (A Focus on the Physical Elements of Systems), #3 (A Focus on Fielded Systems and "Owners & Operators") and #4 (Classes of Entities and Relevant Elements of the Framework).
2	*Question: Do you think current definition of Critical Infrastructure is still fit for purpose?* *CI Definition: 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*
	Response: The current definition is limited in scope to physical parts of the systems - SESA recommends that a holistic systems approach is needed to establish all associated elements that make up the system (its internal architecture in terms of key sub-systems and relationships, resources, processes, tools, information/tech-data) and consider all applicable use-cases in a whole-of-life systems framework (encompassing the system, its key relationships/interfaces, and its enabling support systems). Limiting the scope to just the physical components places at risk the utility and resilience of the CI capability under external (environmental) shock. While the definition helps describe what occurs (impact) in the absence of CI (i.e. having been "destroyed, degraded or rendered unavailable"), it is unclear whether the CI definition is identifying critical sectors, organisations ('entities') or specific assets. The three degrees (sector/CI entities, asset/regulated CI entities, and Systems of National Significance) confound this issue because multiple terms are used at the same level. Note this is exacerbated by the dual use of the term 'CI entity' at both the sector level (CI Entities) and asset level (Regulated CI Entities). Refer also to SESAs general observations #1 (Terminology and Language - "Security and Resilience"), #2 (A Focus on Physical Elements of Systems) and #4 (Classes of Entities and Relevant Elements of the Framework). While the definition helps describe what occurs (impact) in the absence of CI (i.e. having been "destroyed, degraded or rendered unavailable"), it is unclear whether the CI definition is identifying critical sectors, organisations ('entities') or specific assets. The three degrees (sector/CI entities, asset/regulated CI entities, and Systems of National Significance) confound this issue because multiple terms are used at the same level. Note this is exacerbated by the dual use of the term 'CI entity' at both the sector level (CI Entities) and asset level (Regulated CI Entities).

	Refer also to SESAs general observations #1 (Terminology and Language - "Security and Resilience"), #2 (A Focus on Physical Elements of Systems) and #4 (Classes of Entities and Relevant Elements of the Framework).
3	*Question: Are there factors in addition to interdependency with other functions and consequence of compromise that should be considered when identifying and prioritising critical entities and entity classes?*
	Response: Refer previous response (Q#2) - we must consider a "systems of systems" context; establishing the CI systems is a first step that must be followed by establishing the essential relationships required for the CI system to deliver its essential services and the associated management systems that enable these - as it is those management systems that will be critical (as well as common in instances) to ensure resilience and ongoing utility. Refer also to SESAs general comments #2 (A Focus on Physical Elements of Systems), and #3 (A Focus on Fielded Systems and "Owners & Operators").
5	*Question: How should criticality be assessed to ensure the most important entities are covered by the framework?*
	Response: Refer previous two responses (Q#3 and Q#5). There is a need for a common (systems) definition of resilience as a reference foundation. Assessment of criticality of entities is not trivial. Solutions would require careful consideration of multi-criteria decision making. Whilst it will be useful to consider each entity's criticality in a standalone manner, it will also be important to consider the behaviour of the entities together, and the critical chain of effects throughout the system(s). Refer also to SESAs general comment #1 (Terminology and Language - “Security and Resilience”).
6	*Question: Which entities would you expect to be owners and operators of systems of national significance?*
	Response: Perhaps a more appropriate question would be what systems would you expect to be identified as Systems of National Significance (SONS)? The focus on the obligations of 'entities' as owners and operators of SONS as opposed to the SONS themselves may make it difficult to achieve the intended outcomes. Since there is not a one to one mapping of entities to SONS, the following situations may occur: i) there may be multiple entities involved as owners and/or operators of SONS e.g. Australian Tsunami Warning System is delivered by Geoscience Australian, Bureau of Meteorology and Crisis Communications Centre, as well as service providers that these entities rely on. ii) entities that are owners/operators of a SONS may have infrastructure that is not related to the SONS. This infrastructure does not require the level of protection afforded to SONS. Refer also to SESAs general comments #1 (Terminology and Language - “Security and Resilience”) and #3 (A Focus on Fielded Systems and "Owners & Operators") The focus on the obligations of 'entities' as owners and operators of SONS as opposed to the SONS themselves may make it difficult to achieve the intended outcomes. Since there is not a one to one mapping of entities to SONS, the following situations may

	occur: i) there may be multiple entities involved as owners and/or operators of SONS e.g. Australian Tsunami Warning System is delivered by Geoscience Australian, Bureau of Meteorology and Crisis Communications Centre, as well as service providers that these entities rely on. ii) entities that are owners/operators of a SONS may have infrastructure that is not related to the SONS. This infrastructure does not require the level of protection afforded to SONS. Refer also to SESAs general comments #1 (Terminology and Language - "Security and Resilience") and #3 (A Focus on Fielded Systems and "Owners & Operators")
8	*Question: What might this new TISN model look like, and what entities should be included?*
	Response: We recommend the inclusion of SESA, Simulation Australasia, and other pertinent cross-domain/sector technical societies of Engineers Australia (e.g. Asset Management Council or Risk Engineering as well as those societies related to specific critical infrastructure sectors).
9	*Question: How else should government support critical infrastructure entities to effectively understand and manage risks, particularly in relation to cross sector dependencies? What specific activities should be the focus?*
	Response: We recommend Government working with CI entities to help establish essential enabling support relationships applicable across all CI entities and focusing efforts on the health of these. In broad terms, the enhanced framework will require alignment of governance processes and policies around these CI entities and the health of their essential enabling relationships. Information dissemination and flow through the network will be important, but also feedback assessments/auditing of adherence and assurance will be essential. Is it being used by the right people, for the right effect? There will be multiple stakeholders involved within and across different sectors; from government, sector regulators, and owners and operators. Development of systems architectures alongside the enhanced framework can support the understanding of these different perspectives for integration. Government support should not wholly mechanistic or transactional, there is a need to consider the organisational issues of collaboration too as well as ensuring that the various risk management systems and techniques that organisations use interface with this centralised risk management system.
10	*Question: Are the principles sufficiently broad to consider all aspects of security risk across sectors you are familiar with?*
	Response: Security risk is one hazard or source of adversity that needs to be monitored. It should be clarified if the intention is to scope resilience to only security, or whether the framework and principles should encompass a broader set of hazards to the resilience of Australia's critical infrastructure (for example, page 3 states economy and sovereignty in addition to security; and page 4 includes natural disasters and COVID-19). Within Principle 3, it should be clearer that risk is not just about communicating to affected customers, but also to other dependent entities of the framework in a timely manner. Further, the principles need to be applied across a whole-of-life perspective,

	engineering resilience into the design and development of new / modified systems and ensuring the ongoing design-integrity through their useful operational life as well as protecting fielded systems from new / emerging threats. Refer also to SESAs general comments #1 (Terminology and Language - "Security and Resilience") and #3 (A Focus on Fielded Systems and "Owners & Operators").
11	*Question: Do you think the security requirements strike the best balance between providing clear expectations and the ability to customise for sectoral needs?*
	Response: If the framework is broader than security, then consider including obligations related to resilience of CI Capability Systems such as: a) Reliability and availability targets; b) The requirement to conduct (and report on) regular resilience assessments; c) The requirement to perform (and report on) regular disaster recovery testing (including through simulations were appropriate); and d) The requirement to mitigate all identified Single Points of Failure (SPOF) and ensure adequate levels of physical (and functional) redundancy exist. Refer also to SESAs general comments #1 (Terminology and Language - "Security and Resilience") and #3 (A Focus on Fielded Systems and "Owners & Operators").
16	*Question: The sector regulator will provide guidance to entities on how to meet their obligation. Are there particular things you would like to see included in this guidance, or broader communication and engagement strategies of the regulator?*
	Response: There is a possible issue in the reliance on sector regulators as this may inadvertantly promote a siloed approach. Within different entities and systems, there will be more than one sector regulator that may be applicable; assets that fall into one regulator's jurisdiction may find more relevant guidelines in another regulator area e.g. rail signalling might fall under Transport Sector Group rather than the Communications Sector Group and therefore be governed by DHA rather than DITRDC. It will be important to consider how assets and capabilities fall under which regulator(s), and ensure that regulator requirements are consistent and non-contradictory. As noted in earlier responses (Q#3, Q#5, Q#6), the focus needs to be on not just the CI entities, but the health of their essential enabling relationships, and these will most likely be (a) shared in instances across CI entities, and (b) subject to management by other (CI) entities. Refer also to SESAs general comments #1 (Terminology and Language - "Security and Resilience"), #3 (A Focus on Fielded Systems and "Owners & Operators") and #4 (Classes of Entities and Relevant Elements of the Framework).
17, 18 & 19	Question: Who would you consider is best placed to undertake the regulatory role for sectors you are familiar with? Does the regulator already have a security-related regulatory role? What might be the limitations to that organisation taking on the role?
	Question: What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?
	Question: How can Government better support critical infrastructure in managing their security risks?
	Response: See Q#16 response
23	*Question: What information would you like to see shared with industry by Government? What benefits would you expect from greater sharing?*

	Response: While much information regarding the CI sectors and CI assets is in the public domain, it would be useful to create and make available a register of capability systems (i.e. those systems identified as Systems of National Significance and the systems within Regulated CI Entities (referred to in the Act as CI Assets). This register should identify both the system, and the boundaries of each system (inclusive of socio-technical elements e.g. medical workers), to avoid ambiguity, and their essential enabling relationships. Refer also to SESAs general comments #1 (Terminology and Language - "Security and Resilience"), #3 (A Focus on Fielded Systems and "Owners & Operators") and #4 (Classes of Entities and Relevant Elements of the Framework). Refer also to SESAs general comments #1 (Terminology and Language - "Security and Resilience"), #3 (A Focus on Fielded Systems and "Owners & Operators") and #4 (Classes of Entities and Relevant Elements of the Framework).
24	Question: What could you currently contribute to a threat picture? Would you be willing to provide that information on a voluntary basis? What would the cost implications be?
	Response: There could be a benefit in establishing a traffic-light style dashboard showing the status of the CI Capability Systems (Systems of National Significance and systems owned/operated by Regulated CI Entities).
25	*Question: What methods should be involved to identify vulnerabilities at the perimeter of critical networks?*
	Response: There is no definition provided for "critical networks", so this may be intended in the generic sense (e.g. energy networks) or specifically communications networks. Refer also to SESAs general comment #1 (Terminology and Language - "Security and Resilience").
27	*Question: What information would you like to see included in playbooks? Are there any barriers to co-developing playbooks with Government?*
	Response: Identification of each CI systems associated essential enabling relationships. Refer also to SESAs general comments #1 (Terminology and Language - "Security and Resilience"), #3 (A Focus on Fielded Systems and "Owners & Operators") and #4 (Classes of Entities and Relevant Elements of the Framework). Refer also to SESAs general comments #1 (Terminology and Language - "Security and Resilience"), #3 (A Focus on Fielded Systems and "Owners & Operators") and #4 (Classes of Entities and Relevant Elements of the Framework).
28	*Question: What safeguards or assurances would you expect to see for information provided to Government?*
	Response: Active governance (regulation) on protection of security and privacy of the information so provided.
31	*Question: Who should oversee the Government's use of these powers?*
	Response: We recommend the establishment of a Board of Governance with membership to be selected from across CI Entities, enabling entities and cross-domain enabling societies (such as SESA, Simulation Australasia, Risk Society, etc). See also Q#8

34	*Question: What safeguards and oversight measures would you expect to ensure the necessary level of accountability for these type of powers?*
	Response: The refinement outlined in earlier responses of applying a systems approach that helps identify essential relationships and focuses on these will minimise the risks of individual systems owners / operators making unilateral decisions that may not be in the best interest of society. See also Q#31 and refer to SESAs general comments #1 (Terminology and Language - "Security and Resilience"), #3 (A Focus on Fielded Systems and "Owners & Operators") and #4 (Classes of Entities and Relevant Elements of the Framework). See also Q#31 and refer to SESAs general comments #1 (Terminology and Language - "Security and Resilience"), #3 (A Focus on Fielded Systems and "Owners & Operators") and #4 (Classes of Entities and Relevant Elements of the Framework).