Australian Government
Civil Aviation Safety Authority

Comments by CASA on the Consultation Paper (CP)
Protecting Critical Infrastructure and Systems of National Significance (August 2020)
by the Australian Government, Department of Home Affairs, Critical Infrastructure Centre.

CASA takes the opportunity to make the following general comments on this change initiative to "introduce an enhanced regulatory framework" (ERF) the purpose of which is to ensure "that Australia's approach to protecting critical infrastructure is fit for purpose for the modern age" and protects the "essential services that are crucial to our way of life" from a "range of security hazards" (physical, personnel and cyber) (CP, p.1) that could potentially impose unacceptable *societal risk* (consequence-likelihood):

a) **On Security Hazards vis a vis Other Hazards**
While the focus of this ERF is on security hazards, the design and operation of the new framework should work synergistically with extant regulatory frameworks for other types of hazards that can lead to similar levels of societal risk**.**

b) **On Rights and Obligations:** Any changes to the extant regulatory framework -- be them in law, regulation, advisory material, related definitions, etc, and particularly on rights and obligations of public or private organisations and/or the assets and/or services these may deliver, own or control-- should be demonstrably traceable (i.e. via relevant cause-consequence analysis) and proportional to *the societal risk* that would result from the degradation of *essential services* via the effect that the occurrence of the potential security hazard would have on the *critical infrastructure.*

In other words, ultimately the degree of security and consequent rights and obligations should not be tied to the nature/sector of the organisation (public, private, transport, banking, etc.) or the nature/location of the asset (software, hardware, space, ground), but to the *societal risk* resulting from the degradation of the related *essential service* should the hazard eventuate and affect the *critical infrastructure*.

c) **On Security and Safety:** CASA requires organisations to have an appropriate Safety Management System (SMS). Security breaches can lead to adverse safety outcomes. Therefore, CASA expects that the implemented SMSs include appropriate institutional interfaces with the security responsibilities of an organisation. By institutional interfaces we mean, for example, that in managing the safety (security) risk of a potential security (safety) breach, an organisation should take into account all the risk controls that are already part and parcel of complying with security (safety) obligations.

d) **Societal Risk of Position, Navigation and Timing (PNT) Services**: PNT could be said to rely on *critical infrastructure,* which is defined very broadly as "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" (CP, p.11).

Note is made that the *societal risk* of a potential degradation of PNT Services is not driven by the type/location of their supporting technology (e.g. radar, satellite, earth, space, etc.) but by the extent and conditions under which these services are used, and by the resilience of the overall system of systems underlying such services.

For example, the societal risk of the landing service (Navigation) offered at any one airport depends on how busy such airport is (e.g. Sydney vs Hobart), the prevailing weather (e.g. poor or excellent weather all year round), and the number and variety of fall-back systems supporting such service (one only, more than one, ground only, ground with space back-up, etc.).

e) Sector Specific Requirements

The Consultation Paper indicates that Government is especially keen to hear from eleven specific *sectors* that are regarded as fundamental to our society (CP, p.3), and also envisages the possibility of sector-specific requirements (CP, p.4).

In developing the ERF further, analysis and attention should be paid to the fact that whatever the societal risk of an essential service, not all sectors, and not all parts within a sector, contribute equally. This is central to ensuring that any changes brought about by the ERF remain proportional to the societal risk.

For example, *definitions* whose role is to clarify which *changed requirements* will now apply to organisations due to the organisations' potential contribution to societal risk (e.g. through the assets, systems, networks, etc. these organisations may supply, own or control), should include explicit reference to such societal risk and do so in a manner that will enable demonstration via relevant cause-consequence analysis, that the *changed requirement* is necessary and proportional to reduce to the societal risk to acceptable levels.

As an example of the above point of view for the Space Sector, a definition like the following would not suffice to define a 'Critical Infrastructure Asset' for the purposes of 'Government Assistance',

> Assets, systems or networks involved on a commercial basis in the manufacturing, operation or supply to earth stations, earth receive stations, space stations, space receive stations and Australian space objects.

and would need adaptation by, for example:

- appending
  - where the roles of such assets, networks, or systems is such that their potential malfunction due to a security breach would lead to [Catastrophic, Major, Medium, Minor, etc.…] societal risk, in the absence of any other simultaneous malfunction by any other asset, network or system.

- specifying the meaning of 'commercial basis.'

Also for the Space Sector and similarly to the above case, a definition like the following would not suffice to define a 'Regulated Critical Infrastructure Asset' for the purposes of being subject to a 'Positive Security Obligation',

> Assets, networks or systems owned or operated by an entity holding a earth licence, earth receive licence, space licence, space receive licence; or a launch facility license and or Australian launch permit under the Space (Launches and Returns) Act 2018.

and would need adaptation by, for example:

- appending the same text as appended in the previous case;
- adding "excluding class licenses" after "space receive license."