



15 September 2020

Department of Home Affairs  
[ci.reforms@homeaffairs.gov.au](mailto:ci.reforms@homeaffairs.gov.au)

## **PROTECTING CRITICAL INFRASTRUCTURE AND SYSTEMS OF NATIONAL SIGNIFICANCE – SUBMISSION IN RESPONSE TO DISCUSSION PAPER**

CSIRO welcomes the opportunity to participate in the *Protecting Critical Infrastructure and Systems of National Significance* consultation. This is an important topic, both for CSIRO and the national Innovation system.

CSIRO has legislated responsibility for a range of research facilities that could be considered ‘critical infrastructure’ under the definition presented in the discussion paper. In addition, CSIRO provides access to research facilities and associated services in conjunction with a range of collaborators in the broader research and innovation sector, which also have direct relevance to Australia’s critical infrastructure. CSIRO also undertakes research and develops technologies that may constitute systems of national significance.

This submission provides general comments related to the criticality of research facilities and highlights the financial impact to collaborating organisations if they are required to adjust their business model to comply with higher standards.

We would be pleased to meet with the Department to discuss these matters further.

### **The Criticality of Research Facilities**

CSIRO considers that some of its research facilities should be identified as critical infrastructure. The global and domestic events of 2020 have particularly highlighted the criticality of our research facilities.

As examples, Australia could not have progressed research and testing of the virus and vaccine candidates in response to the COVID-19 pandemic without access to CSIRO’s Australian Centre for Disease Preparedness (ACDP) in Geelong and CSIRO’s Protein Production Facility at Clayton.

ACDP is unique in Australia. It is a national Level 4 biocontainment facility operated by CSIRO on behalf of the Australian Government. As the highest level of biological safety, a Level 4 laboratory provides the necessary level of security to enable work with highly dangerous and exotic microbes. Infections caused by these types of microbes are frequently fatal, and often come without treatment or vaccines. ACDP is one of only a handful of labs of this kind in the world and the only one in the southern hemisphere.

CSIRO staff at ACDP have undertaken ground-breaking research which has assisted Australia’s response to the pandemic and added to global knowledge about the virus. Importantly these facilities have been used as part of Australia’s partnership with the Coalition for Epidemic Preparedness Innovations (CEPI).

CSIRO's Protein Production Facility is critical to growing supply of vaccine candidates to be tested by ACDP or vaccines for domestic manufacture by industry and have been critical to work by CSL and other key players. Both facilities are unique in the southern hemisphere and are critical to Australia's response and in our preparedness for future pandemics.

Also, during the summer, the Canberra Deep Space Communications Centre run by CSIRO under contract to NASA was under threat from bushfires. The Centre is one of three globally that form NASA's deep space communications network. NASA formally wrote to CSIRO to remind us that the facility is considered a critical facility by the US Government.

### **Cyber Security Standards Issues for Critical Infrastructure**

Research and research facilities are collaborative by nature and this poses some challenges particularly in relation to cyber security. As these collaborations/consortia are formed with a range of organisations such as businesses, government agencies, not for profits and international organisations, the application of consistent cyber standards is an issue. If a research facility is deemed critical infrastructure, the issue of what standards and to what level they are applied will need to be resolved.

As an Australian Government agency, CSIRO works to meet the Government's standards for cyber protection. Where CSIRO is the host institution, our policies apply to that facility and so our cyber security standards also apply. However, given the collaborative arrangements of the research facilities, there may be instances where it will take time and resources to align with these standards and this may be a barrier for some collaborators.

CSIRO recommends this rule is adopted as a consistent approach for all critical infrastructure. Further, to develop consistent standards of cyber protection, CSIRO recommends that if research infrastructure is considered critical, then the Australian Cyber Security Centre should work with host organisations to determine the application of appropriate cyber security standards.

### **Research Infrastructure and Costs**

The Australian research community relies on the communications network delivered by the Australian Academic Research Network (AARNet). AARNet is a not for profit entity wholly owned by 38 universities<sup>1</sup> and CSIRO. Given the importance of AARNet to the research community CSIRO believes that the AARNet network could be considered as critical infrastructure for Australia. This would then have implications for the security standards applied to the network.

Research organisations will be required to change their business model in order to meet higher cyber security standards, which will create additional new costs for universities and collaborators. The financial impact of this should be considered as policies for critical infrastructure are developed.

### **Broader impacts for the research sector**

CSIRO notes that in the application of a new policy:

- regulatory burdens should be distributed evenly across the research sector;
- any new regulations related to research should align with and not duplicate existing regulations required of government research agencies;
- the research work of Publicly Funded Research Agencies (PFRAs) may be inadvertently impacted by new regulations on our research partners, including universities and industry due to, for example, mismatches in cyber standards between PFRAs and universities;
- facilities funded under the National Collaborative Research Infrastructure Strategy (NCRIS facilities) may be best served by following the regulatory requirements of their host institutions; and
- NCRIS and other funding programs will need to take on board the costs of new business models and of the requirements for higher levels of cyber protection.

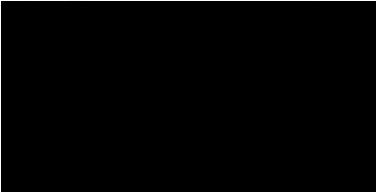
---

<sup>1</sup> <https://www.aarnet.edu.au/about-us/governance/shareholders/>

It is also important to highlight the risks to industry should facilities fail or become unusable due to lack of compliance. A failure to comply could be the result of confusion and/or lack of capability which could be skills or costs based. This is because the compliance checking process will not be trivial. For this reason, some form of automation in compliance checking and conformance would be beneficial for both regulation enforcing entities and critical infrastructure entities.

Thank you again for the opportunity to provide input to your considerations. If you require any further information, please contact Elizabeth Yuncken at [REDACTED] or [REDACTED].

Yours sincerely

A large black rectangular redaction box covering the signature area.

Judith Zielke  
Chief Operating Officer