Protecting Critical Infrastructure and Systems of National Significance Consultation Paper Feedback

16 September 2020

sta.org.au
ABN: 71 626 822 845

Science & Technology Australia thanks the Department of Home Affairs for this opportunity to provide feedback on its proposals on protecting critical infrastructure and systems of national significance.

STA respects the need to safeguard Australia's critical infrastructure and notes the role of our research, education and innovation sectors as nationally significant institutions.

STA is concerned, however, by the growing weight of the regulatory burden on Australia's universities and research institutes, and the prospective imposition of further costs to fulfil additional reporting responsibilities.

The cost of additional reporting requirements would be even more challenging at a time when universities are reeling financially from the loss of billions of dollars in revenue and thousands of job losses amid COVID-19. No additional financial assistance has been made available by Government at this time.

In our view, many of the security considerations outlined in the consultation paper are already covered extensively under procedures and regulations currently in place. These include but are not limited to:

- Protocols and relationships developed through the University Foreign Interference Taskforce; and
- Reporting requirements under the Defence Trade Controls Act 2012.

We do not see any clear evidence to suggest Australian universities and research institutions such as medical research institutes need further regulation beyond the already strong systems in place.

Relevant procedures and regulations

In response to the specific issues outlined in the discussion paper, STA highlights two regulatory processes that already cover security arrangements across much of Australia's research and innovation sector.

The Defence Trade Controls Act 2012 (which was reviewed as recently as 2018) and the Guidelines to Counter Foreign Interference in the Australian University Sector, co-authored in an equal partnership between the university sector and Government and national security agencies in 2019.

Universities also have access to the current security intelligence and protective security advice from the Australian Security Intelligence Organisation's Business and Government Liaison Unit. Universities are in regular contact with these units to share information on risks and seek additional information as they manage those risks.

University Foreign Interference Taskforce

The security of our national infrastructure is not a static challenge. It is the subject of ongoing adaptation as new threats and risks emerge. It is in the spirit of this evolving landscape that the University Foreign Interference Taskforce was formed last year as an equal partnership between the university sector and agencies of Government.

This taskforce includes representatives of the university sector and representatives of Australian Government Departments including Home Affairs, Education, Attorney-General's, Defence, and the Australian Security Intelligence Organisation. Our of the work program of four specialist working groups that fed into the taskforce, a set of guidelines and best practice principles were developed and released in 2019 to assure the security of Australia's research and research infrastructure.

The Guidelines to Counter Foreign Interference in the Australian University Sector were designed to enable ongoing consultation and updates of shared security practice in a more flexible and nimble approach than heavy-handed red tape or regulation. Such an approach means universities can regularly address new risks to their systems and research infrastructure based on rapid advice from taskforce members based in national security agencies. STA sees this taskforce as a more effective protective measure than additional legislation that will increase regulatory burden without the rapid response and mutual partnership approach that this taskforce has established.

Defence Trade Controls Act 2012

The research and education sector also understands that systems of national significance need to astutely safeguard the unintended export of technologies and innovations which could have a potential defence or security application for foreign powers or foreign actors. Through the Defence Trade Controls Act, sensitive research and innovation with a potential 'dual use' application must be assessed in consultation with the Department of Defence. Feedback from the Department has

historically been that Australia's research institutions tend to over-report rather than under-report technologies that could potentially fall under tis legislation out of an abundance of caution in the national interest.

The list of technologies covered by this legislation is updated every year when the latest Defence and Strategic Goods List is tabled in Parliament.

Regulatory burden

The research and education sector takes its national security responsibilities seriously. At the same time, there is an undeniable cost to the growing weight of the regulatory burden imposed on institutions like universities. Increasing regulations and reporting eat into the funds that can be invested in the nation's leading-edge research. This is not to say sensible and proportionate risk management is not needed, but rather that regulation should not seek to double up on work already being undertaken on a voluntary partnership between research institutions such as universities and national security agencies.

Safeguarding national security and protecting critical infrastructure is a fluid challenge. To effectively protect large systems of national significance like universities, an approach that fosters a partnership between universities and national security agencies is a strong model. Such partnerships enable the adoption of best practice quickly and with minimum regulatory cost and burden to institutions.

Support for universities to manage cybersecurity risks

While the mechanisms outlined above deliver substantial protective measures to Australia's research sector, there is always room for improvement. There is no doubt that cybersecurity is a continuous focus for universities around both education and research.

The discussion paper proposes that Government assistance will be provided as part of any additional regulatory requirements on institutions such as universities and medical research institutes. This acknowledgement is welcome – however, universities and research institutes already face substantial regulatory burden with the current measure in place. The government assistance outlined in this paper comes in the form of directions and direct actions, rather than funding to cover the costs of additional staff time and systems that may be required to report in an additional formal regulatory environment.

We thank you for your attentive consideration to our feedback on behalf of the nation's science and technology sectors.

Yours sincerely,

Associate Professor Jeremy Brownlie
President
Science & Technology Australia

Misha Schubert
CEO
Science & Technology Australia