



Queensland University of Technology

Response to the exposure draft of the *Security Legislation Amendment (Critical Infrastructure) Bill 2020*

Queensland University of Technology (QUT) welcomes the opportunity to comment on the exposure draft of the *Security Legislation Amendment (Critical Infrastructure) Bill 2020*.

QUT endorses the Universities Australia (UA) submission to the present consultation. We support UA's recommendations in their entirety, to wit:

1. *The Government consult in greater detail with the university sector before introducing the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (the bill) to Parliament. A sector-wide working group would be an appropriate mechanism.*
2. *That the legislation, as it applies to the university sector, should be proportionate and workable, risk-based and carefully targeted.*
3. *That Government should develop a robust regulatory impact statement prior to the introduction of the bill to Parliament.*
4. *That Government should work with the university sector in developing an implementation timeframe that matches the maturity of the sector and takes into account the level of financial investment.*
5. *That the Government consider better coordination across Commonwealth departments and agencies on national security and associate matters in the university sector, to ensure a coherent, cohesive and efficient approach.*

We would like to expand a little on the import of the final recommendation, because there are emerging concerns across the sector about a lack of coordination and mutual awareness across Government with respect to the application national security and foreign influence measures to universities.

The university sector absolutely recognises the seriousness and importance of protecting Australia and its public institutions – including universities – from untoward and pernicious foreign influence, interference and injury. We also appreciate the gravity of national security matters, and the delicacy with which they must be addressed, including the need for secrecy. Our concern does not go to the policy objective of securing Australia: it goes to implementation.

It is apparent from recent experience that various parts of Government are initiating measures to protect universities from foreign interference without regard for each other's proposals, let alone for the existing rigorous collaborative arrangements that are already in place. We consider it most unlikely that federal agencies would wilfully ignore related initiatives or effective existing measures, so we can only conclude that there is a lack of knowledge and understanding of what other parts of Government are doing to address concern in this arena.

The *Security Legislation Amendment (Critical Infrastructure) Bill 2020* proposed by Home Affairs is a leading example, coming very soon after another example, the *Australia's Foreign Relations (State and Territory Arrangements) Bill 2020* and its associated

consequential amendments Bill, brought by Foreign Affairs. Both proposals seem to have been drafted in apparent ignorance of the effective operation of the University Foreign Interference Taskforce (UFIT), established by the Minister for Education and chaired by a Deputy Secretary of the Department of Home Affairs.

If the Commonwealth does not address this lack of coordination and line of sight between agencies and better integrate initiatives designed to counter foreign interference, there are three likely adverse effects that will result:

1. A counterproductive elevation of underlying risk

Most seriously, this uncoordinated approach will produce an increase in real terms to our sector's *de facto* exposure to foreign influence, interference and malevolent attack, as universities' resources are engaged increasingly in addressing multiple overlapping but differently designed compliance protocols, with excess attention and energy devoted to rechecking every corner and ticking boxes instead of watching the gate. These overlapping compliance obligations will be the responsibility of the same officers – the effect in operational terms will be a reduction of monitoring effectiveness as multiple compliance elements are ticked off under several paradigms to cover broadly the same monitoring and scrutiny activity.

Vigilance will suffer unless we can instead agree on a set of common activities, protocols, concerns and measures that cover all needs with good visibility for all relevant interested parties. We have a far greater likelihood of achieving the overarching policy objective of protection from harm under a single overarching regime that meets everyone's needs than through a collection of poorly conceived, uncoordinated and blunt instruments, which is the current scenario. The Commonwealth designed UFIT to be just this kind of effective, flexible and collaborative mechanism – characterised by the sharing of good practice and the maintenance of a synoptic view of the security environment and of areas of concern – yet the Government is now introducing entirely new regimes (such as those from DFAT and now Home Affairs) as though UFIT does not exist.

The reduction in functional vigilance due to an increase in bureaucratic compliance that adds significant labour but marginal additional scope of attention is especially true in the reduced staffing environment now characteristic of universities in light of the financial effects of COVID-19. While adding compliance complexity for little to no gain is never a good idea, universities are simply not in a position at present to devote additional resources to meet the additional non-productive burden.

2. Tension with other Government policy priorities

The lack of coordination has policy implications as well as the potential to hamper operational effectiveness. Some of the measures being proposed are antithetical to and actively antagonise other initiatives and priorities of Government, such as the protection of academic freedom, the encouragement of university-industry collaboration, and the imperative to conduct world-class research.

3. Unnecessary regulatory impact

Each of the new regimes proposed DFAT and Home Affairs appears to have been designed in isolation, as though it were the only one addressing concerns in this domain, with the result that the mechanism in each case is both blunt and far too broad, with an unnecessarily outsized regulatory impact. A net this large will not only harvest an enormous by-catch, it is also the wrong instrument to catch the subtle and alert target – surely a major priority of national security concern. Departments should be made aware

of existing effective measures such as UFIT, the *Defence Trade Controls Act 2012* and the like, enabling them to ensure their specific concerns are met by addressing any gaps in that work to ensure the unified regime is proportional, efficient and effective, instead of arbitrary, laborious and ineffectual.

QUT proposes that the remedy is an effective inter-agency collaboration mechanism, combined with broader membership of UFIT, to identify, harmonise and develop protection regimes to ensure all concerns are addressed. The *Security Legislation Amendment (Critical Infrastructure) Bill 2020* should be redrafted to integrate the critical infrastructure protection requirements into the work of UFIT, in consultation with that Taskforce and the sector broadly. If gaps are identified in protocols and practices, they should be addressed through UFIT, rather than establishing an entire new regime to run in parallel.