Australian Government
Department of Education

Report on implementation of the Guidelines to Counter Foreign Interference in the Australian University Sector

August 2023

Contents

Executive Summary

Context

Australia's higher education system is recognised for its quality global engagement and consistent research output. International collaboration is fundamental to this success, and the *Guidelines to Counter Foreign Interference in the Australian University Sector* (the Guidelines) are in place to ensure this engagement continues while protecting Australia's national interests. All Australian universities are in the process of implementing measures to protect their operations while continuing to build strong research and organisational partnerships.

The University Foreign Interference Taskforce (UFIT) was established in 2019, bringing together the university sector and Australian Government agencies to support an environment of trust and resilience. The UFIT provides guidance to support universities' decision-making based on proportionate risks, so Australian universities can continue to produce world-class research. The UFIT Steering Group acts as the primary conduit for all counter foreign interference related activities involving collaboration between universities and government.

The Guidelines were originally established in 2019 as a collaboration between the Australian Government and the university sector to uplift the foundational elements essential for building awareness of, and resilience to, foreign interference within a university. The Guidelines were refreshed in 2021 to reflect the changing risk landscape and offer specific and measurable actions that universities could apply, building upon the significant work undertaken by the university sector to implement measures since 2019.

On 7 September 2022 the Hon Jason Clare MP, Minister for Education, outlined that the government would undertake a comprehensive university sector consultation to better understand the successes and challenges of implementing the refreshed Guidelines.

The Department of Education (the department) invited universities to engage with this consultation process through roundtable discussions and questionnaires, seeking insight into the different approaches universities have taken in their application of the Guidelines. The department consulted other government agencies involved in implementation of the Guidelines and the broader national security ecosystem as part of the consultation process.

There was significant engagement from the sector, with all Australian universities opting to participate and articulate the substantial work they have undertaken in implementation. The department received questionnaire responses from all 42 universities, and responses to a separate questionnaire from 4 peak bodies. There were 101 sector attendees at the university consultation roundtables; separate one-on-one discussions were held with 9 government agencies.

Key findings

Since the refreshed Guidelines were released in 2021, all Australian universities have taken active steps to implement the Guidelines. In 2022, following a Department of Home Affairs-led consultation process on the implementation of the Guidelines, vice-chancellors of all 39 member universities of Universities Australia confirmed an understanding of the threats posed by foreign interference, and progress in implementing advice in the Guidelines.

As per the design of the Guidelines, this implementation varies in extent and maturity, proportionate to the level of risk faced by each university. In the 2023 consultations, the sector emphasised that each university has a unique risk profile and that there is no one-size-fits-all strategy for managing foreign interference. The sector continues to support the Guidelines in their current form, in particular the voluntary nature of the underpinning framework and proportionality to risk.

Implementation of the Guidelines was supported across the breadth of all universities. There is a particular depth of engagement at senior levels, and work is ongoing in the sector to embed this engagement at the practitioner level, within research units and the student body. Consultations demonstrated that as universities become cognisant of emerging risks facing the sector, there may be benefits to sharing training resources, best practice examples and case studies, particularly to enhance communication of risks to the student body.

Some universities have gone beyond what is outlined in the Guidelines, understanding they may be more susceptible to certain risks and have sought to address this accordingly. This is particularly relevant to cybersecurity, where universities recognise the whole-of-enterprise risk of a cyberattack and have implemented safeguards beyond those referenced in the Guidelines. Work to improve universities' protection against vulnerability to cyberattacks will need to be ongoing as risk landscapes continue to evolve.

The consultations identified that universities acknowledge implementation of the Guidelines is not a 'point-in-time' endeavour. Universities noted the risk environment continues to change and countering foreign interference is an ongoing process that requires adaptability and evolution in approach. Universities noted that more frequent and specific information sharing from government would support ongoing implementation of the Guidelines, to ensure adherence with the Guidelines is appropriate, proportionate and timely.

The consultations demonstrated the value of collaboration and partnership between the sector and government, and that there is continued opportunity for government and the sector to work together. Improvements in knowledge and information sharing, more training resources and annual reporting of the sector's progress on implementation all provide opportunities for collaboration in the future.

Methodology

In early 2023, the department took a two-stage approach to consult with the sector, engaging in face-to-face and virtual discussions with universities, as well as providing universities and peak bodies the opportunity to respond to a short questionnaire. 42 Australian universities[1], 8 peak bodies[2] and 9 government agencies were invited to take part in this process.

The two-stage approach allowed for quantitative data collection through questionnaires, and for universities to detail their unique processes for implementation. The consultation roundtables enabled open and free discussion between the sector and the department, providing opportunity for universities to elaborate on some of the issues raised.

Sector consultation roundtables

Overall, **101** people engaged in the sector consultation roundtables, representing all 42 invited universities. The department held 5 in-person consultation roundtables across Australia, hosted at various universities. Three additional consultations were held virtually. Details of these sessions are noted below:

Location	Date	Number of Attendees
Sydney, NSW Host: The University of Sydney	Thursday 16 March 2023	12
Brisbane, QLD Host: Queensland University of Technology	Wednesday 22 March 2023	10
Canberra, ACT Host: The Australian National University	Friday 24 March 2023	10
Perth, WA Host: Curtin University	Wednesday 29 March 2023	15
2 x virtual sessions Microsoft Teams	Friday 31 March 2023	43
Melbourne, VIC Host: La Trobe University	Tuesday 4 April 2023	8
Virtual session: University of Sunshine Coast Microsoft Teams	Monday 17 April 2023	3

1 Pursuant to the Tertiary Education Quality and Standards Agency (TEQSA) National Register of Australian universities: National register search | Tertiary Education Quality and Standards Agency (teqsa.gov.au)

2 Pursuant to the Austrade 'Study Australia' peak bodies: Government and peak bodies - About Austrade Education - For Australian education institutions - Austrade

The Counter Foreign Interference Coordination Centre (CFICC) at the Department of Home Affairs (Home Affairs) was invited to attend the consultation sessions, with Home Affairs' representatives in attendance at Canberra, Perth, Melbourne and virtually. Group of Eight and Universities Australia were also invited to attend all sessions. Group of Eight attended the Canberra session.

Questionnaire

On 16 December 2022, the Deputy Secretary Higher Education, Research and International, wrote to 42 vice-chancellors, peak bodies and government agencies foreshadowing this consultation process. This was followed by distribution of an online questionnaire in February 2023.

The questionnaire distributed to the university sector contained 20 questions, mapped to the 4 pillars of the Guidelines as well as the threat context and broader national security considerations.

The questionnaire distributed to peak bodies posed 6 questions, seeking feedback from peak bodies on their reflections of best practice, key challenges and emerging themes from their member base.

The department received completed questionnaires from all 42 universities invited to respond and completed questionnaires from 4 peak bodies.

Government agency views

Concurrently, the department also facilitated individual discussions with 9 government agencies involved in supporting the sector's implementation of the Guidelines or broader national security frameworks.

Details of these sessions are noted below:

Government Agency	Date of Consultation
Tertiary Education Quality and Standards Agency	Thursday 23 February 2023
Australian Research Council	Friday 3 March 2023
Attorney General's Department	Thursday 9 March 2023
Australian Cyber Security Centre	Friday 10 March 2023
Australian Security Intelligence Organisation	Monday 20 March 2023
Department of Foreign Affairs and Trade	Tuesday 21 March 2023
Department of Home Affairs	Monday 3 April 2023
Department of Defence	Monday 17 April 2023
Department of Education (internal)	Thursday 27 April 2023

Findings from consultations

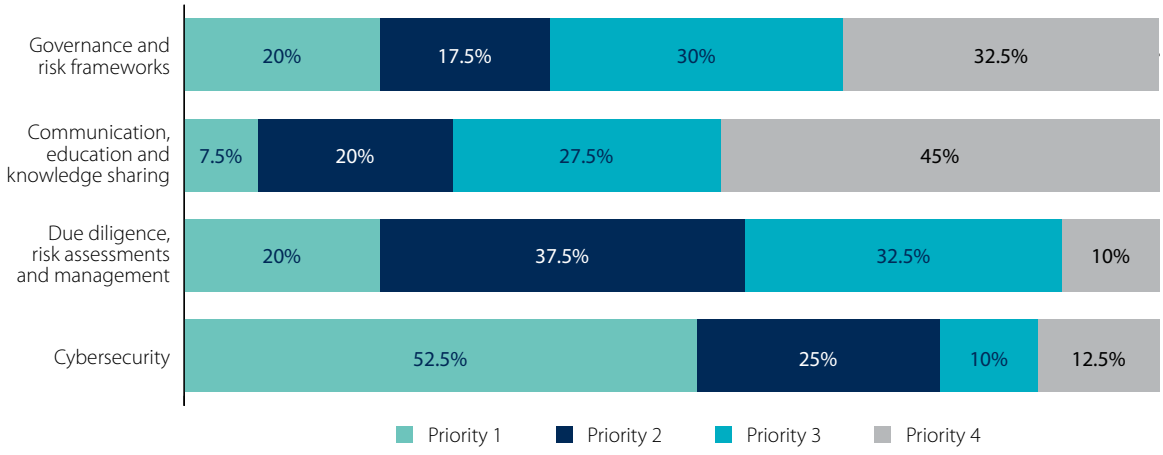
Consultations demonstrated that all Australian universities are engaging with the Guidelines and are implementing measures to protect themselves against the risk of foreign interference. Further, the sector is broadly pleased with the form and function of the Guidelines and appreciate the importance of an underpinning framework in protecting universities from risk and ensuring consistent aims among different approaches.

Consultations demonstrated an array of approaches to implementation, proportionate to the unique circumstances of each university. There is a high degree of willingness to work in partnership with the government to continue implementing risk management strategies. Universities demonstrated an appreciation of the seriousness of the threat of foreign interference and the importance of active risk mitigations to protect staff, students and research.

The consultations focused on the four pillars of the Guidelines:

- Governance and risk frameworks;
- Communication, education and knowledge sharing;
- Due diligence, risk assessments and management; and
- Cybersecurity.

Figure 1. Feedback from Universities in ranking each pillar of the Guidelines by priority (investment of time, energy and resources).



The overall response in the government consultations was also generally positive. All government agencies highlighted the extent of work to date undertaken by the university sector in implementing the Guidelines. Agencies indicated that there are benefits to regular reporting on the Guidelines from the sector to reflect ongoing

opportunities for engagement between the sector and government, and to demonstrate universities' ongoing work on implementation. Feedback received regarding the work of the UFIT has also been mostly positive, however some universities not represented have commented on a lack of visibility of current considerations being undertaken by the UFIT Steering Group.

Threat context

The sector reported their understanding that there are unique threats facing universities, staff and students, and are all actively engaged in efforts to protect themselves from risk. There is appetite for further partnership between government and the sector to support detailed discussion on the threat context and ensure universities are appropriately informed of risk and have an avenue to discuss specific scenarios.

The implementation of the Guidelines has raised awareness in the sector of the risks that they are faced with, and provided a framework for universities to manage their risk with a proportionate approach. Throughout the consultation process, it was clear that universities have awareness of the different types of risk facing the sector, including the different types of foreign interference that can occur on campus, with implications for information holdings, staff, students and research.

Spotlight: Improving university-wide understanding of the threat context

In recognition of the importance of understanding the threat context, the Office of the Chief Security Officer at one university has undertaken substantial responsibility for risk identification and understanding the broad threat context. This university has also identified and established various foreign interference accountable authorities, tasked with different aspects of implementing the Guidelines and uplifting understanding of foreign interference throughout the university.

Successes

- At a senior leadership level, there is a strong awareness of the threat context and risks facing universities, and investment to continue to collaborate with government on approaches to counter foreign interference.
- The sector has embedded sound approaches to risk management into operational decision making at the middle management and practitioner level.

Challenges

- Universities noted a lack of clarity about what sort of foreign interference has relevance to the university sector, and believe the government could strengthen support through more specific threat information or examples to inform university decision making.
- Some smaller universities noted the challenges of receiving, providing and sharing classified information due to the absence of security cleared individuals across the university.
- Some government agencies noted that while universities are being asked to implement the Guidelines proportionate to risk, there is a risk that some universities may underestimate their risk to cyberattacks or foreign interference.

National security ecosystem

The Guidelines exist within a broader national security ecosystem, including other resilience mechanisms and legislative requirements, such as the Foreign Arrangements Scheme and the Foreign Influence Transparency Scheme, that protect Australia's national interests. All universities implement these frameworks, working with government departments and other organisations to meet their obligations. The Guidelines are also a key mitigation and quality assurance tool considered by the Australian Research Council (ARC) and the National Health and Medical Research Council.

Throughout the consultation process, both the sector and government agencies noted that greater whole-of-government coordination with respect to foreign interference issues could reduce duplication of efforts. A number of agencies proposed clearer communications on particular roles of government agencies and operating legislation, and information on contact points would be useful to streamline engagement between government and universities. This need for greater clarity extends to feedback regarding reporting obligations with respect to the various tools, such as the Australian Security Intelligence Organisation's Notifiable Incidents, Threats or Reportable Observations (NITRO) portal and the Australian Cyber Security Centre, as universities were looking for greater direction on who to report incidents to.

Successes

- Some universities reported that implementation of the Guidelines, as well as compliance with other national security legislation, has led to an overall increase in visibility of foreign and international arrangements held across the university.
- The Guidelines provide a practical framework from which universities can operate, and due to their voluntary nature, do not lead to overlap with government legislation.
- Universities reported positive interactions with their respective state-based Department of Home Affairs CFICC staff.
  - Universities noted that productive discussion and engagement with government agencies stemmed from having pre-existing professional networks and connections with government.

Challenges

- Some universities commented on the challenge of different government reporting and overlapping legislative requirements, with the number of different contact points and agencies burdensome to staffing resources and time.
  - This was also raised as a challenge in reporting foreign interference, as universities are sometimes unsure which mechanism to report through.
- Some universities expressed that the Guidelines are written as though they are mandatory, rather than voluntary, as each section does not preface that universities *could* consider each action.
  - Universities commented that in the course of seeking grant funding from certain bodies, universities are required to indicate compliance with the Guidelines. This is inconsistent with the voluntary nature of the Guidelines.

Governance and risk frameworks

Most universities already had broad and overarching compliance and risk frameworks in place prior to the release of the Guidelines. As universities have gained more awareness of the risks that face the sector, in part due to the Guidelines, many have established more rigorous governance and risk frameworks or specific foreign interference related risk management resources, that help to manage foreign interference risk. Throughout the consultation process, universities reported comprehensive frameworks, processes and procedures that are in place to manage risk.

Spotlight: Integrating countering foreign interference into existing policies

The Guidelines encourage universities to consider how their frameworks and policies identify and mitigate threats of foreign interference, and promote, support and strengthen resilience. One university has reported uplifting its entire suite of internal policies and procedures to address foreign interference risks, rather than developing a standalone policy. This university conducted a comprehensive review of its policies and how they were working across the university, and determined that a singular policy would not suit their environment due to the overlap in responsibilities across different parts of the university.

Instead, this university has implemented foreign interference-specific procedures which document and guide university staff regarding what to do in the event they are engaging in certain activities, or encounter particular risks. These procedures also outline contact points across the university and refer staff to where they can find further guidance material.

Spotlight: Foreign interference oversight/advisory committee

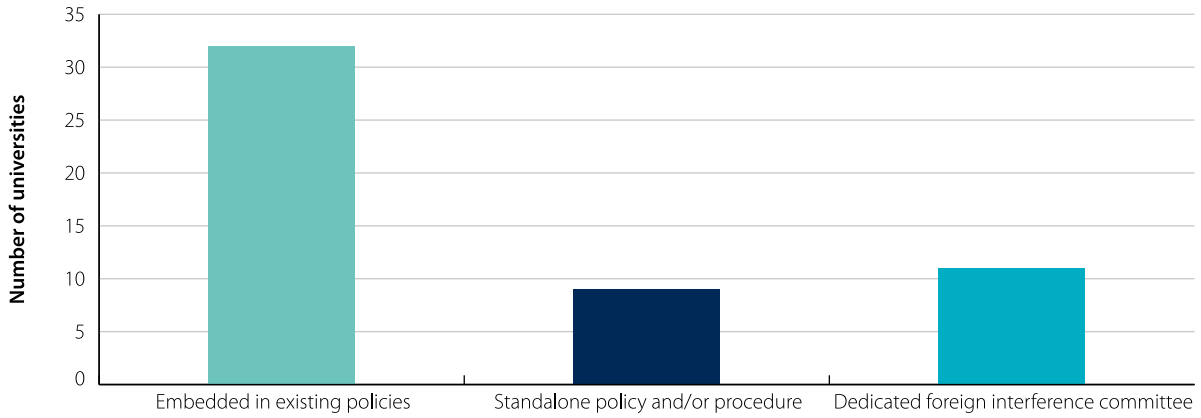
The majority of universities reported that foreign interference risks are monitored through existing audit and risk committees, but a small number of universities advised that they had established a foreign interference-specific advisory or oversight committee.

One university in particular has established a foreign interference–specific advisory committee, which includes membership from across all relevant sections of the university. This committee's role is to provide overarching support and governance on mitigating the risks associated with foreign interference in the university's activities.

Successes

- Most universities reported that the increase in risk management frameworks and development of supporting in-house guidance materials has resulted in a heightened risk awareness across the university, not just related to Guidelines implementation and international collaboration.
  - Multiple universities reported establishing foreign interference oversight or advisory committees which bring together staff from different areas of the university, ensuring that implementation is not siloed.

Figure 2. How universities address foreign interference through governance and risk frameworks.
Note: some universities have both standalone policies and dedicated committees.



Challenges

- Some universities reported that it was challenging to measure success of risk frameworks and at times, emphasise the extent of the risk across the organisation, due to the clandestine and at times indistinguishable nature of foreign interference.

Communication, education and knowledge sharing

Key to successful implementation of the Guidelines has been an uplift in understanding of what risks face the sector and how this knowledge can best be shared. With the release of the Guidelines in 2019 and the 2021 refresh, universities have gained more awareness of the risks that face the sector and have implemented training to ensure their staff are adequately informed and prepared to manage these risks. Ongoing training should ensure information shared is relevant and timely. While many executive and senior staff at universities are engaged in countering foreign interference, some parts of the sector commented on the need for education and knowledge sharing to occur at all levels of staff, and amongst students.

Universities were widely supportive of the training tools prepared and provided by government, and other workshops and forums to help further this education in the sector. Case studies were mentioned as being particularly useful for universities in enabling them to better understand how risk could present itself.

Successes

- Many universities have reported an increase in cross-sector collaboration and communication, including the sharing and collaboration of resources, as a result of implementation of the Guidelines.

Spotlight – Western Australia community of practice

Some universities based in Western Australia have taken steps to form a community of practice to discuss countering foreign interference in their universities. Relevant practitioners meet virtually on a quarterly basis to share resources, discuss current issues and challenges impacting the sector and their region, and to develop and maintain a network of contacts and colleagues with knowledge of risk management in the university sector.

Member universities cited that this forum was particularly useful following the commencement of the *Foreign Arrangements Scheme*, with universities sharing their approach to addressing the registration obligations and related administrative functions.

- Almost all universities who engaged in the consultation process already have training mechanisms in place for staff, particularly those who engage in research; some universities are also extending this to ensure students are aware of the risks, particularly higher degree by research (HDR) students.
  - Those universities that do not currently have training in place have identified this is a current consideration.
  - As the sector matures in its understanding of countering foreign interference, some universities are looking to develop resources that better encompass the shifting risk landscape.

Challenges

- Many universities have found it challenging to communicate the risks of foreign interference to staff and students.
  - In particular, some universities cited challenges in sensitively communicating with staff and students in such a way that did not unduly raise fears or encourage divisiveness. As a result, many universities are not able to offer specific training for both staff and students, instead only focusing their efforts on staff (see figure 3).
  - Further, where some universities offer specific training to students, they often encounter challenges providing tailored training to HDR, PG and international students (see figure 4).
- Many universities commented that the need to develop in-house training and guidance materials was burdensome on time and financial resourcing.

Figure 3. Number of universities that provide specific foreign interference training for staff and/or students.

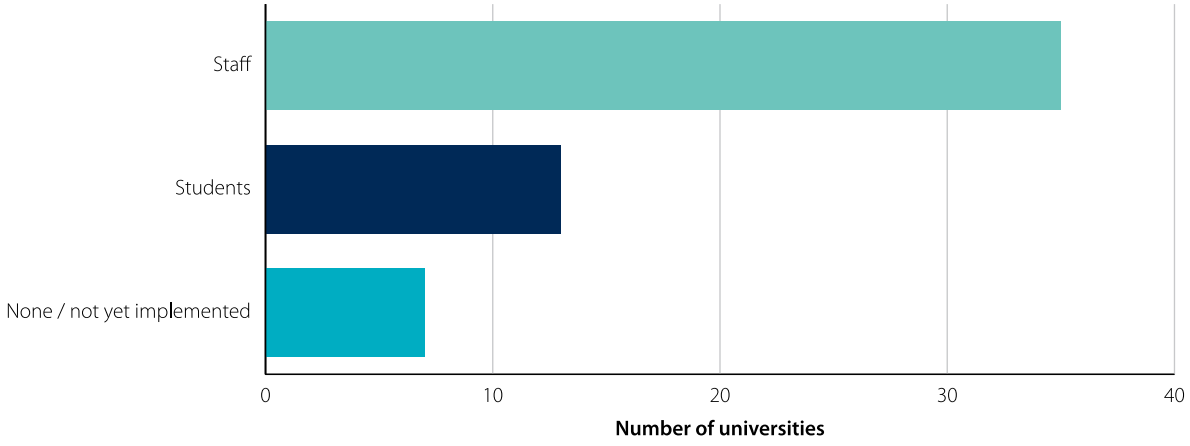
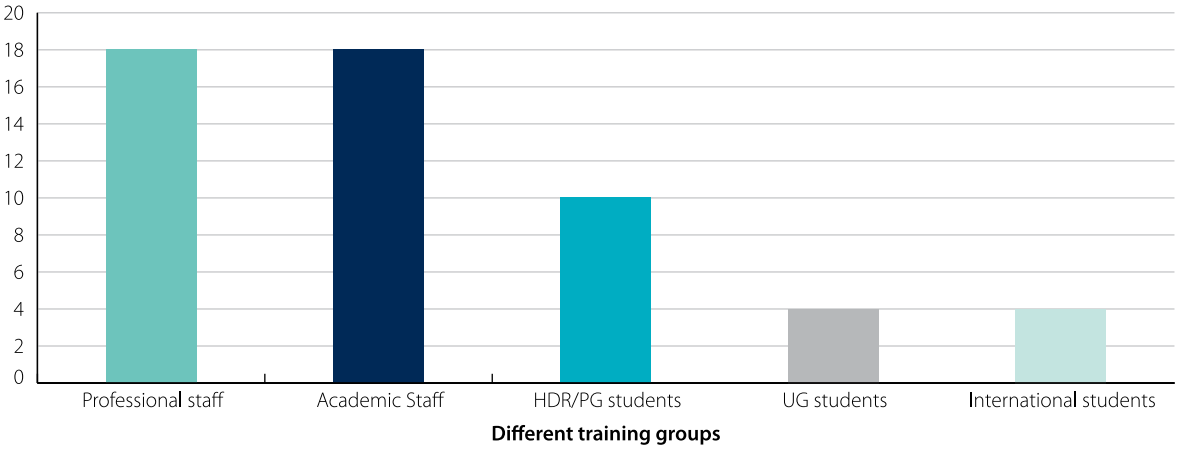


Figure 4. Where universities indicated that they provided training to staff and/or students and further information was provided in responses, this graph breaks down the number of universities delivering training to specific types of staff or the student body.



Due diligence, risk assessments and management

The sector has demonstrated significant progress in processes around due diligence and declarations of interest since the release of the Guidelines, which is supported by improved knowledge and understanding of the risks facing the sector. Universities are continuing to refine their due diligence tools and processes and acknowledge that this work will be ongoing.

Successes

- The majority of universities have approval, audit and continuous evaluation mechanisms in place, focused on assessing and managing foreign interference risks and vulnerabilities.
  - Universities without these in place largely reported other mechanisms to ensure this security, such as risk frameworks not directly tied to foreign interference.
- Universities have reported significant improvements in conflict and declarations of interest processes.
  - While not used solely in instances of identifying risks to the sector, these tools are of use for general due diligence and increased risk awareness.

Spotlight – 'Declarations' of interest

Most universities reported requiring staff to complete some form of conflict of interest declaration. A number of universities however have reported a cultural shift away from 'conflicts' of interest, and towards defined 'declarations of interest', citing that staff are generally not in a position to assess their own interests as being conflicting.

These universities also reported that 'declaration' better supports their efforts in enhancing transparency culture within the university, as it is a more positive term. Further, one university reported that the cultural shift towards 'declarations', on a voluntary basis, has resulted in over 85% compliance by all staff.

Challenges

- While universities have improved their conflict and declaration of interest processes, some have reported a need for more guidance regarding what to do with the information received.
- Some universities have struggled to develop appropriate due diligence tools in house and have had to seek support from external consultants. This can result in reduced capacity within the university and financial costs for the university.

Cybersecurity

Cybersecurity remains an issue at front of mind for the sector. Given the risk of cybersecurity incidents and the broad scale impact a cyberattack could have, universities are particularly attuned to the risks they face. Throughout the consultation process, the sector continued to report high levels of engagement in cybersecurity, with many universities reporting that their cyber compliance is more advanced than what is outlined by the Guidelines. Universities will need to be agile in ensuring protection against cyberattacks and adapt to changes in risk, noting that this response will look different for each university proportionate to their level of risk.

Feedback collected by Home Affairs in mid-2022 revealed that the sector were investing most of their efforts into 'communication, education and knowledge sharing' and 'due diligence, risk assessments and management'. The department's consultations demonstrated that universities have since channelled focus and resourcing into cybersecurity, making it the top priority for investment when compared against the other pillars. Universities reported that investment in cybersecurity provides greater benefit than solely protecting against foreign interference, drawing links between why these priorities have shifted.

Successes

- The Guidelines have increased awareness of the importance of cybersecurity in the university sector and have provided advice particularly to smaller universities who may not have been as advanced as larger universities.
- The Guidelines frame cybersecurity as a 'whole-of-organisation risk', encouraging a whole-of-organisation approach in addressing potential issues. This holistic approach encourages the protection of all of the systems at risk.
- The majority of universities noted that cybersecurity was the pillar of the Guidelines most heavily invested in.

Spotlight – Cybersecurity strategies and roadmaps

The Guidelines encourage universities to implement a cybersecurity strategy that treats cybersecurity as a whole-of-organisation human issue and incorporates an appropriate controls framework. Many universities have reported either having developed, or significant progress towards the development of, an institutional cybersecurity strategy.

One university has reported having developed a strategy and supporting roadmap to direct the ongoing investment and maintenance of its cybersecurity capabilities. This strategy and roadmap also dictate regular reviews of the threat landscape in which the university is operating. Further, this work is guided by a specific risk appetite for cybersecurity, which is used to direct the cybersecurity program of work to achieve the level of risk mitigation required, proportional to the original threat assessment.

Spotlight – Specific cybersecurity information sharing platforms

Most universities reported being members of, or involved in, at least one forum specific to the sharing of information on cybersecurity across industry and the sector. The identified platforms include the Council of Australasian Universities Directors of Information Technology (CAUDIT), Australasian Higher Education Cybersecurity Service (AHECS), the Joint Cyber Security Centres (JCSC) or the Trusted Cyber Security Forum (TCSF).

A number of universities also reported the use of externally provided security operations centre (SOC) capabilities offered through the Australian and Academic Research Network (AARNET), who provide the university sector with enhanced detection and response capabilities, developing and practising incident response plans and playbooks, and running leadership and operational tabletop exercises.

Challenges

- Many universities reported that their cyber compliance goes beyond what is outlined in the Guidelines based on contemporary requirements and incident management approaches, and that they do not tend to rely on the Guidelines risk mitigation approaches when it comes to cybersecurity.
- Universities noted an organisational, reputational and business risk precluding the sharing of cyber-incident occurrences and discussion on incident response
- Some universities reported that threat modelling is not being implemented due to a lack of resources or cyber maturity.

Opportunities

Ongoing work will be required to ensure the Australian university sector continues to implement enduring protections to counter the risk of foreign interference. This will be best managed through strong existing partnerships between government and the sector, including the University Foreign Interference Taskforce.

Threat context

- Specific and frequent information sharing between government and universities, to ensure the sector has the most relevant information on risks they face.

Cybersecurity

- Sharing of threat modelling techniques, approaches to cybersecurity and lessons learned as an opportunity for capacity building across the university sector and ongoing discussion as the risk evolves.

National security ecosystem

- Increased and regular discussion between government agencies to ensure consistent and streamlined outreach to the sector.
- The development of a roadmap that outlines all national security legislation that applies to the university sector, including contact points for responsible agencies within government for the sector.
- The completion of annual surveys on ongoing implementation of the Guidelines by the sector, to ensure ongoing work and support provided by government adapts to a contemporary context.

Governance and risk frameworks

- The development of a flowchart of recommended next steps universities can take in the event of a suspected or actual instance of interference on campus, which captures approaches to internal and external reporting that apply to both staff and students.

Communication, education and knowledge sharing

- The development of further training materials and risk communication plans, tailored to different demographics (e.g. specific to academic and professional staff, undergraduate/postgraduate students, HDR students).
- The establishment of sector-wide communities of practice specific to foreign interference, with membership at practitioner/officer level, to encourage sharing of resources across the sector.
- Targeted workshops and seminars, including focused thematic sessions for smaller regional universities, to ensure ongoing upskilling and training for those within the sector.
- Collaboration between the sector and government on the development and provision of additional case studies, including best practice examples, to better inform universities of what risk can look like.

Due diligence, risk assessments and management

- The creation of a central register of declarations of interest for researchers, to ease the administrative burden for researchers moving between universities.
- The development of a tool for conducting foundation-level due diligence checks, which can be adapted to meet the needs for each university.
- Change in terminology from 'conflict of interest' to 'declaration of interest' to encourage transparency across universities.