GUIDELINES TO COUNTER FOREIGN INTERFERENCE IN THE AUSTRALIAN UNIVERSITY SECTOR

University Foreign Interference Taskforce

ACKNOWLEDGEMENTS

The University Foreign Interference Taskforce Steering Group members are acknowledged for their contributions to the development and refresh of the *Guidelines to counter foreign interference in the Australian university sector (Guidelines)*. In addition to the Steering Group, the three working groups established under the Steering Group, co-chaired by an Australian Government and a sector representative, expertly drafted content on agreed key strategic areas for these refreshed *Guidelines*.

The university sector's ongoing participation and extensive collaboration throughout the process is acknowledged.

The *Guidelines* were developed in October 2021.

Australian Government

UNIVERSITIES AUSTRALIA

GROUP OF EIGHT AUSTRALIA

CONTENTS

INTRODUCTION

The world-class performance and reputation of Australia's university system is intrinsically linked to the globally engaged and open nature of our universities.

Universities play a key role in developing new knowledge and technological innovation. This role is vital to Australia's continued prosperity and economic growth. Deep international engagement, underpinned by university autonomy and academic freedom, fosters the sharing and developing of knowledge with the best and brightest minds around the world.

The Australian Government supports international collaborations through its programs and policy settings across a wide range of initiatives and portfolios.

This crucial global engagement is occurring in an ever more complex and evolving world. It is essential that universities, the community and government have confidence that proportionate strategies are in place to manage the risks to Australia's university students, staff and research. This is also important for international partners seeking assurances when working together on sensitive topics.

Universities and government are working together to enhance current protections, while preserving the openness and collaboration that is crucial to the success of Australia's world-class university system.

Universities conduct research within a wide array of fields: from the arts to social sciences, from health and medical sciences to engineering and information technology. It is important to maintain a sensible approach that is proportionate to the risk.

Proportionality of risk underlines the *Guidelines*

The vast majority of the university sector's international interactions benefit Australia, and the *Guidelines to counter foreign interference in the Australian university sector* (Guidelines) are not intended to inhibit academic activities that are low risk.

Australian universities rely on a regular flow of communication to and from security agencies to support their strategies to mitigate the risk of foreign interference. The Australian Security Intelligence Organisation (ASIO) assesses that espionage and foreign interference continue to pose a threat to Australia, its sovereignty and the integrity of its national institutions.

Australia's university sector is one of the sectors at risk in our community, given it is at the leading edge of policy, research and scientific development. Its work leads to the development of proprietary and other sensitive information critical to the development of new technologies, medicines, techniques and practices that are fundamental to Australia's social and economic prosperity.

The majority of university international interactions are positive and benefit Australia.

However, there are those who seek to interfere in the university sector. This can manifest itself as seeking to inappropriately influence course content, research directions, and student and staff actions.

The compromise of valuable research, or other sensitive data, could cause significant and long-term damage to Australia through the loss of intellectual property (IP) and commercial advantage. It could also lead to potential damage to reputation and international standing, and Australia's economy and national security. Attempts to inappropriately influence academic discussions or public statements made by members of the university community can lead to self-censorship, and conflicts with the principle of academic freedom.

All universities are subject to foreign interference risks but their risk profiles will vary depending on the nature of the activities they undertake – for example, universities with significant research programs may be at a higher risk of unwanted technology transfer. Other universities may be at higher risk of challenges to academic freedom.

The *Guidelines* recognise these differences and encourage universities to adopt measures to mitigate foreign interference risks that are appropriate to their particular risks. Transparency is the key to countering foreign interference.

A proactive approach by the university sector to the threat of foreign interference helps to safeguard the reputation of Australian universities, protect academic freedom, and ensure our academic institutions and the Australian economy can maximise the benefits of research endeavours.

Such a response is consistent with Australia's approach to countering foreign interference, which aims to increase the cost and reduce the benefit to those conducting foreign interference in Australia.

‘Foreign interference’ versus ‘foreign influence’

Foreign interference

Foreign interference occurs when activities are carried out by, or on behalf of a foreign actor, which are coercive, clandestine, deceptive or corrupting and are contrary to Australia’s sovereignty, values and national interests.

Foreign influence

All governments, including Australia’s, try to influence deliberations on issues of importance to them. These activities, when conducted in an open and transparent manner, are a normal aspect of international relations and diplomacy and can contribute positively to public debate.

How foreign influence could cross the threshold into foreign interference

Simply voicing support for a particular government or its policies is not, of itself, foreign interference. If that advocacy is secretly directed by, or covertly done on behalf of, a foreign government, however, and is contrary to Australia’s national interest, it crosses the threshold into foreign interference.

Protest activity on Australian university campuses can be a healthy sign of a democratic society. However, if this activity was secretly being directed by a foreign state, or community members had been coerced to participate or prevented from protesting by a foreign state, then it would cross the threshold into foreign interference.

Working in partnership: the University Foreign Interference Taskforce

The higher education sector is working in partnership with government to mitigate risks and promote Australia as an attractive international research and education partner.

The Australian Government and the higher education sector jointly formed the University Foreign Interference Taskforce (UFIT) in August 2019, to enhance safeguards against the risk of foreign interference.

The *Guidelines* released in 2019 are globally recognised as a world-leading innovation to help protect Australian research and education assets in an increasingly complex environment. These refreshed *Guidelines* build upon the substantial progress universities have made since 2019 in their work to increase awareness of, and resilience to, the risk of foreign interference in the Australian university sector. This version continues to recognise universities’ autonomy.

The *Guidelines* seek to strike a balance and give careful consideration to the potential tensions between developing institutional policies that protect against the risk of foreign interference, while also promoting the free exchange of ideas, an open research culture and academic freedom.

Universities have already invested significantly in developing sophisticated risk-management frameworks and associated policies and practices, while upholding the foundational principle of university autonomy. This includes managing risk associated with international collaboration and engagement.

The key themes and objectives to manage and engage with risk and best-practice considerations provided in these *Guidelines* are intended to build upon this base.

The shared objective of both universities and government is to safeguard the security of Australia's university sector without undermining the invaluable asset of its openness, which optimises benefits to our community.

The overarching principles applied when developing and refreshing these *Guidelines* were:

- Security must safeguard academic freedom, values and research collaboration.
- Research, collaboration and education activities remain mindful of the national interest.
- Security is a collective responsibility with individual accountability.
- Security should be proportionate to organisational risk.
- The safety of our university community is paramount.

These *Guidelines* are intended to be applied proportionate to the risk at each institution, and are not intended to introduce unnecessary burdens on universities. Universities are encouraged to consider the *Guidelines*, identify their own highest risks to help prioritise resourcing, and apply mitigations that are appropriate to their specific risks.

The *Guidelines* are not intended to be exhaustive of all considerations for universities about foreign interference risks.

These *Guidelines* contribute to building greater resilience to threats in the Australian university sector, while respecting the importance of global collaboration.

Australian Government agencies will continue to work closely with universities to improve the sector's foreign interference mitigation efforts, including providing support for implementing the principles contained in the *Guidelines*. This support includes:

- briefing university senior executives on threats and national security policy
- raising awareness with university staff of foreign interference
- engaging with universities through ASIO and Counter Foreign Interference Coordination Centre outreach officers who can work with institutions to increase understanding of the foreign interference threat, and ways to respond to those risks
- providing updates to the sector on critical technologies of national interest to Australia
- strengthening university cybersecurity capability and providing guidance on strategies to address cybersecurity incidents through the Australian Cyber Security Centre.

The government also established the ASIO-led Counter Foreign Interference Taskforce which is responsible for conducting investigations and undertaking enforcement activities that relate to foreign interference.

About the *Guidelines*

These *Guidelines* are foundational elements that are essential for building resilience within a university. They are designed to be holistic and reinforce each other. Understanding threats and risks will help drive and build proportionate and calibrated activities to counter foreign interference. A positive security culture within universities is a core component that will help to embed considerations of risk at all levels. Being part of a community of best practice to enable sharing of intelligence and process will promote the resilience of the sector and the nation.

These *Guidelines* support universities to develop new or examine existing tools, frameworks and resources to use for assessing and mitigating risks from foreign interference, proportionate to risk. They also promote greater consistency across the sector.

They offer principle-based and specific advice to universities on how to manage risk in their institution. The advice recognises that risk is not uniform across the sector, and universities may implement additional or existing leading-practice mitigation actions proportionate to their own risks of foreign interference.

Universities are encouraged to consider whether the *Guidelines* can be applied to transnational education business models or offshore campuses, where appropriate.

Sector implementation of the *Guidelines*

These *Guidelines* sit within a wider context that includes Australian Government legislative frameworks such as *Australia's Foreign Relations (State and Territory Arrangements) Act 2020* and the *Defence Trade Controls Act 2012*. Other context and input may be provided through other government processes such as Parliamentary inquiries.

Guidance material developed and compiled through UFIT is available to support universities in implementing the *Guidelines*. This includes government resources and information such as related legislation and codes.[1]

The guidance material provides additional advice, tools, suggested frameworks, references and other materials, including hyperlinks to other government resources.

This material aligns with the themes in the *Guidelines* and will be updated as required to reflect the evolving threat and rapidly changing environment.

Since 2019, many universities have developed leading practices, with policies and actions that take into account their institutional risk profiles, and strengths and priorities proportionate to the risk. These leading practices are shared among the sector.

Reporting requirements

Universities can use the data and reporting generated from adoption of these *Guidelines* to promote their approach to counter foreign interference across the sector and to government in line with university governance processes, for example in university annual reports.

The government may also seek assurance from universities that their approach to counter foreign interference aligns with these *Guidelines* and is proportionate to their risks.

[1] List of legislation and codes is available in the guidance material.

SUMMARY OF THE *GUIDELINES*

Each guideline should be considered by universities proportionate to their risk.

1. Governance and risk frameworks

1.1 Universities have frameworks for managing their risks that address foreign interference threats to their university's people, information and assets.

1.2 Universities have accountable authorities responsible for managing foreign interference risk.

1.3 Universities have policies and procedures that set out responsibilities and expected conduct for all those engaging in their university's business to manage foreign interference risk.

1.4 Universities have clear risk assessment and reporting frameworks available to all staff and students that guide decision-making for activities at risk of foreign interference.

1.5 Universities have transparent escalation and reporting mechanisms for foreign interference-related matters.

2. Communication, education and knowledge sharing

2.1 Universities have communication plans and education programs that raise awareness and support mitigation of their foreign interference risks.

2.2 Universities provide training to staff and students who are engaged in foreign collaboration or other partnership activities at risk of foreign interference.

2.3 Universities participate in sector-wide counter foreign interference events and where appropriate, share experiences and leading practice, to learn from each other and build sector resilience.

2.4 Government supports the sector through raising awareness, sharing information relating to foreign interference and being accessible.

3. Due diligence, risk assessments and management

3.1 Universities require declaration of interest disclosures from staff who are at risk of foreign interference, including identification of foreign affiliations, relationships and financial interests.

3.2 Universities conduct due diligence to inform decision-makers of foreign interference risks.

3.2.1 Universities conduct due diligence on partners and personnel.

3.2.2 Universities assess the potential of technology and/or research.

3.3 Universities apply a comprehensive approach to their due diligence.

3.4 Universities have approval, audit and continuous evaluation of due diligence processes.

4. Cybersecurity

4.1 Universities understand and proportionately mitigate cyber business risks, using techniques like threat models where possible, to inform their cybersecurity strategy.

4.2 Universities implement a cybersecurity strategy that treats cybersecurity as a whole-of-organisation human issue and incorporates an appropriate controls framework.

4.3 Universities participate in communities of best practice, which share cyber intelligence and lessons across the sector and government.

1 GOVERNANCE AND RISK FRAMEWORKS

Identifying and mitigating risk is core to managing foreign interference. The Guidelines are designed so that foreign interference risks can be integrated into existing risk frameworks, policies and procedures. The advice builds on the experience in institutions and the university sector. Universities have existing policies, frameworks, systems and processes, and these help to promote a positive security culture that is proportionate to each university's assessment of its level of risk, and consistent with the principle of university autonomy.

Objective

Universities have frameworks and policies in place to identify and mitigate threats of foreign interference, and promote, support and strengthen resilience.

1.1 Universities have frameworks for managing their risks that address foreign interference threats to their university's people, information and assets.

- Risk frameworks outline the nature of the foreign interference risks, possible mitigation measures and review periods.
- Universities could include foreign interference measures in their regular internal review systems, such as existing internal audit schedules.
- Government provides advice on foreign interference threats to help universities identify and manage risks.

1.2 Universities have accountable authorities responsible for managing foreign interference risk.

- The accountable authority oversees risk and reporting frameworks and that proportionate mitigation strategies are effectively implemented and recorded.
- The accountable authority regularly reviews and communicates security risks and mitigations (relevant to their institution) to university colleagues, government and sector counterparts through appropriate mechanisms.
- The accountable authority oversees foreign arrangements, collaborations and funding.
- The accountable authority oversees university responses to reported issues.
- The accountable authority facilitates regular briefings on foreign interference risk management and issues to the university council (or equivalent).

An accountable authority is a senior executive or executive body, responsible and accountable for the security of people, information and assets to counter foreign interference.

1.3 Universities have policies and procedures that set out responsibilities and expected conduct for all those engaging in their university's business to manage foreign interference risk.

Policies and procedures set out:

- the responsibilities, obligations and expected conduct, and consequences if these are not met
- how universities address foreign interference–related issues such as harassment and intimidation that can lead to self-censorship
- who is responsible for tracking responses, and how these responses to foreign interference-related reports or incidents are managed
- the method and frequency for assessing the effectiveness of security strategy, policies and procedures related to foreign interference, and for updating as needed.

Universities should consider:

- how they regularly communicate with all staff and students about responsibilities and expected conduct relating to foreign interference policies, supports and reporting mechanisms, and the consequences if not met
- how they train and support relevant staff and students to help them understand and respond to foreign interference concerns
- when to share concerns about possible intimidation or undue influence (including by parties external to the university) with government to discuss possible actions and resolutions.[2]

1.4 Universities have clear risk assessment and reporting frameworks available to all staff and students that guide decision-making for activities at risk of foreign interference.

Frameworks set out:

- due diligence processes that consider sources of domestic and foreign investments, partnerships and disclosure of interests, such as foreign affiliations, relationships and financial commitments
- the frequency of due diligence checks, including declarations of interest
- when additional due diligence checks are required
- processes to address concerns raised through due diligence and risk assessments
- risk assessments, mitigations, level of delegation and approval of mitigations, when activity is initially scoped and during the course of the activity
- when and how to review and evaluate project risks and mitigations
- how to manage data, equipment or materials handling and storage.

1.5 Universities have transparent escalation and reporting mechanisms for foreign interference-related matters.

Policies or procedures set out:

- when, how and to whom possible foreign interference-related incidents are reported, both within the university and, as appropriate, to government authorities at either state or federal level
- how staff and students can escalate concerns of foreign interference, through internal processes that maintain confidentiality as appropriate
- how reported concerns are tracked, resolved and recorded, and shared with the accountable authority.

[2] Specific contact details are available in the relevant guidance material.

2 COMMUNICATION, EDUCATION AND KNOWLEDGE SHARING

Universities are communities of staff, students and visitors performing a range of activities that carry a variety of risks, as well as a myriad of benefits. Communication plans and education programs enhance awareness of foreign interference risks for those most at risk in these communities. Promoting a culture of awareness will assist individuals to identify concerns and escalate them as appropriate. This will assist universities to develop a deeper understanding of their risks, and effective mitigations, over time.

There is a challenge in finding the balance between protecting against the risk of foreign interference and promoting the free exchange of ideas, which is a core principle of universities.

Universities and government also share information amongst institutions and sectors. This includes sharing examples of foreign interference such as attempts to exert undue influence or otherwise undermine academic freedoms and values. Security agencies assist universities to identify risks and proportionate responses, including through online resources.

Objective

Universities support a resilient culture in their communities through communication and targeted training that recognises the value of robust exchanges of ideas and global collaboration for our higher education system. Government and universities share knowledge on emerging threats and experiences of foreign interference.

2.1 Universities have communication plans and education programs that raise awareness and support mitigation of their foreign interference risks.

- Universities raise awareness of staff and students by providing access to information about how foreign interference can occur on campus and how to raise concerns within the university or with appropriate authorities.
- Universities promote to all staff and students ways to report within their university concerns of foreign interference, intimidation and harassment that can lead to self-censorship, contrary to academic freedom and freedom of speech. This may include providing information or training during student and staff orientation and induction programs.
- Universities communicate their expectations of appropriate conduct, and consequences if not met, to those using campuses for their own activities, including student associations and hosts of public events.
- Government provides up-to-date and regular information, training and awareness-raising resources, such as through the activities of the Counter Foreign Interference Coordination Centre.

2.2 Universities provide training to staff and students who are engaged in foreign collaboration or other partnership activities at risk of foreign interference.

- Training addresses how to recognise, mitigate and handle concerns of foreign interference, recognising that the experience of their staff can be a valuable resource.

2.3 Universities participate in sector-wide counter foreign interference events and where appropriate, share experiences and leading practice, to learn from each other and build sector resilience.

- Leading-practice examples are shared among the universities' accountable authorities.
- Universities share lessons learned, leading practices and due diligence information within their institution.
- Universities may wish to share leading practices on countering foreign interference with their trusted international partners, to build confidence in collaboration and exchange opportunities.

2.4 Government supports the sector through raising awareness, sharing information relating to foreign interference, and being accessible.

- Government agencies help universities identify instances, or attempts, of foreign interference.
- Government provides points of contact to support universities, for example the Counter Foreign Interference Coordination Centre.

3 DUE DILIGENCE, RISK ASSESSMENTS AND MANAGEMENT

Due diligence helps to identify and assess the level of risk of foreign interference. Transparency is key. Due diligence is conducted before the start of any activities at risk of foreign interference, and is regularly reviewed in accordance with university policies and procedures. Universities seek to develop a culture of continual disclosure.

Working with those whose legal systems and approaches to academic freedom and human rights do not align with our own, carries a higher risk of exposure to undue influence or acts. Critical and emerging technologies are also potentially at higher risk of foreign interference. These risks, if not mitigated, can adversely affect an individual, a university or even Australia's economic, social or national interests. However, global engagement is also crucial to these interests, so government and universities will continue to work to find a balance between openness and protection. International affiliations can bring value to research and other activities, and should not be viewed as a barrier to engagement. Transparency allows appropriate risk mitigation to be put in place where risks are identified.

Comprehensive risk assessment and consideration of mitigation strategies can reduce exposure to, and the likelihood of, foreign interference while maintaining the ability to engage internationally. To support informed decisions, universities have a strong management framework in place to comprehensively consider risk, and apply controls, processes or procedures that guide the proposed research activity or international collaboration.

Objective

Universities promote transparency as a foundational requirement for staff engaging in international partnership activities and collaborations.

3.1 Universities require declaration of interest disclosures from staff who are at risk of foreign interference, including identification of foreign affiliations, relationships and financial interests.

- Universities determine which staff are asked these questions in accordance with a university's assessment of its risk.
- Declarations of interest are collected in accordance with university policies, for example annually, with additional disclosures declared when circumstances change.

Declaration of interest policies or procedures set out:

- core declaration of interest questions [Appendix]
- declaration obligations (which may be layered according to level of risk)
- how additional scrutiny should be applied to those interests identified as higher risk
- how declarations are stored to provide a holistic assessment of risk
- the escalation pathways in place for when conflicts are identified
- how conflicts and declarations are monitored, managed and reported internally.

Identifying risk does not preclude an activity from proceeding.

Declaring international associations or affiliations allows the management and mitigation of potential risks.

3.2 Universities conduct due diligence to inform decision-makers of foreign interference risks.

- Due diligence is conducted on research activities, partners, and university staff and research students who are at risk of foreign interference.
- Due diligence informs a range of university decisions, including applications for national competitive grants and other Australian Government funding.

3.2.1. Universities conduct due diligence on partners and personnel.

Additional checks to further assess and understand potential partners and personnel where indicated by identified risk, may include:

- ownership structure and management
- controlling interests
- business registration
- background
- board members and directors
- history of legal issues
- issues pertaining to IP rights
- the relative ranking of partners in the proposed area of research (Who leads in the proposed area of research?).

3.2.2. Universities assess the potential of technology and/or research.

Additional checks to assess the potential use and risk of technology and/or research where indicated by risk assessment may include:

- the potential uses of the technology or research (noting this can take years to become apparent with a new technology, or may emerge during the research)
- whether the research is an attractive target, for example, where Australia is a world leader
- the technology readiness level
- the potential commercial value
- whether the technology area is captured within Australia's Defence Strategic Goods List (DSGL) and therefore regulated for physical export or electronic supply beyond Australia
- additional compliance checks such as autonomous sanctions and other relevant legislative frameworks
- the possible impact on the diversity or competitiveness of markets and supply chains.

Such assessments, including changes to the sensitivity level of a given technology during the course of a research project, can be complex. Government departments and security agencies provide support to universities for this activity.

3.3 Universities apply a comprehensive approach to their due diligence.

To strengthen due diligence approaches universities:

- have a clear point of contact (for example, a research, risk or international specialist) from whom researchers and staff can seek advice or support when assessing and managing foreign interference risks for university activities
- have a clear point of contact within specialist government security agencies or departments when additional advice or information is required
- consider additional protection measures when there is an assessed increased risk – for example, potential IP leakages or ownership confusion can be mitigated by a plan for commercialisation, or licensing of current and emerging technologies
- include processes to guide decision-makers to review the ethical and reputational risks involved
- where appropriate, consider whether staff appointed by the partner institution should also be accountable to a senior staff member in the institution.

Where appropriate, agreements with international partners:

- affirm the primacy of Australian law and the university's written policies over the law of the foreign partner institutions for all relevant activities taking place in Australia
- address potential threats to the integrity of the research and reputation of the university
- identify emerging or potential foreign interference and security risks that can reasonably be foreseen at the time
- demonstrate the ability to protect information and technologies (for example, through a security management plan)
- incorporate regular ongoing reporting, engagement and review points
- articulate IP ownership and IP transfer
- include termination clauses for non-disclosure or providing false information.

3.4 Universities have approval, audit and continuous evaluation of due diligence processes.

Processes include:

- ways to escalate review of higher risk activities for approval by a university authority or body that can make a decision based on the comprehensive risk assessment and proposed mitigation strategies. This body weighs the risks and opportunities outlined in a proposal
- continuous evaluation of risk and risk-mitigation strategies.

To assist with approval, audit and continuous evaluation, universities:

- conduct due diligence reviews and regular risk assurance updates where appropriate
- revisit ongoing arrangements over time, including assessments of partners, as appropriate and proportionate to the risk
- review arrangements annually to assess new risks and potential vulnerabilities that may have emerged during a foreign collaboration
- request assurance that activities under an arrangement have ceased when a decision is made not to renew – for example, removing access to university systems by the relevant collaborators and requesting any material be returned
- seek to ensure provisions in an original agreement specify steps that must be taken by both parties if the collaboration arrangement ceases.

4 CYBERSECURITY

Universities can be vulnerable to cyber attacks due to their size, complexity and intrinsic openness. University networks are diverse, holding vast data repositories, complex research systems, education platforms, and bespoke Internet of Things (IoT). They also host students and staff and their personal devices, including those offshore, both on campus and remote.

The level of risk, and therefore the level of response that each university will need, varies across the sector. Some universities will face a higher level of risk, depending on the range and focus of their activities, and all universities should consider how resources are prioritised against their risks. Cybersecurity programs can be complex, requiring initiatives extending over multiple years and implemented in a staged and proportionate manner.

Australian universities have increasingly moved to remote learning and research environments to retain and protect students and staff. This shift has meant a broader digital footprint.

Building a positive cybersecurity culture should be a core component of a university cybersecurity strategy.

These *Guidelines* are consistent with *Australia's Cyber Security Strategy 2020* and will assist government to identify how best to partner with universities (both as autonomous institutions and as members of a sector) to enhance cybersecurity across the sector. They are not intended to replace the wealth of detailed technical guidance available from the Australian Cyber Security Centre (ACSC) and other trusted sources.

Objective

Universities protect information systems against unauthorised access, manipulation, disruption or damage, and seek to assure their confidentiality, integrity and availability.

4.1 Universities understand and proportionately mitigate cyber business risks, using techniques like threat models where possible, to inform their cybersecurity strategy.

- Threat modelling is used as a method to help universities identify potential threats, map them to business risks, and feed into cybersecurity strategies and cybersecurity investment plans.
- Threat models for the circumstances of individual universities can leverage useful examples from other universities.
- Government, for example through ACSC, provides regular guidance to enhance understanding of the nature of the threats faced.

4.2 Universities implement a cybersecurity strategy that treats cybersecurity as a whole-of-organisation human issue and incorporates an appropriate controls framework.

Cybersecurity strategies:

- are informed by threat models where possible, based on a best-practice controls framework, and articulate success measures
- help guide investment in, and sustainment of, a group of interrelated capabilities covering people, processes, technology and infrastructure that is proportionate to risk
- should help drive broader transformation to protect against recurrence of incidents and assist universities to meet emerging threats.

Cybersecurity strategies set out:

- security policies, standards, guidelines and procedures
- security roles and responsibilities
- a digital identity management component
- measures for supporting assets, addressing vulnerability and managing threats
- key cybersecurity objectives and controls
- training and awareness programs
- business continuity planning and disaster recovery
- business risks arising from cyber threats.

4.3 Universities participate in communities of best practice, which share cyber intelligence and lessons across the sector and government.

Sharing allows:

- universities to develop a common picture of threats and respond more quickly to them
- government to provide more timely tailored assistance, and better contribute to the success of the higher education and research system, in line with the goals of the *Australia's Cyber Security Strategy 2020*.

APPENDIX

Declaration of interest questions

Universities should determine which staff are asked these questions in accordance with a university's assessment of its risk. Universities should also ensure compliance with relevant legislation, such as that enacting the Foreign Influence Transparency Scheme and the Foreign Arrangements Scheme. Both require notification to government regarding foreign arrangements and affiliations.[3]

1. **Are you receiving any financial support (cash or in-kind) for education or research related activities from a country other than Australia? If yes:**
   - Specify the country.
   - Name of the organisation.
   - Provide a summary of the type of financial support (e.g. name of funding program, period of the funding, type of support received).
2. **Do you hold a position (paid or unpaid) or honorific titles in any foreign university, academic organisation or company, or are you under any other obligations to a foreign university, academic organisation or company (e.g. membership of a talent recruitment program)? If yes:**
   - Specify the country.
   - Name the organisation who provided the position or title.
   - Provide a summary of the position, including any obligations associated with the title.
3. **Are you associated or affiliated with a foreign government or foreign military, policing or intelligence organisation? If yes:**
   - Specify the country.
   - Name the organisation.
   - Provide details of each association/affiliation (e.g. dates and nature of the affiliation).

For Question 2 where there is an elevated risk of foreign interference, including where a researcher is engaged with sensitive technologies, the staff member should address the prior 5 year period.

Risk assessment approaches vary in maturity across the sector, and universities may be assisted by the use of best practice models. Some universities have developed processes which can assist in applying questions in a manner that is proportionate to risk. The University of Queensland's approach provides such a model for universities to consider. It uses three tools to collect information on potential conflicts of interest, secondary employment and sensitive research, applied in a manner proportionate to risk. The use of such a model can be adapted to take account of each university's specific circumstances, and would enable universities to provide specific and measurable responses as requested to do so by government. Universities will share leading practice examples, including through mechanisms provided by their peak body, Universities Australia.

[3] See *Foreign Influence Transparency Scheme Act 2018*, Part 2. See *Australia's Foreign Relations (State and Territory Arrangements) Act 2020*. The Act defines universities that are established by, or under, the laws of a state or a territory as a State/Territory entity (Division 2, Section 7(e)); and specifically includes the Australian National University under the terms of the Act (Division 6, Section 55). As universities are not included in the definition of core State/Territory entities (Division 2, Section 10), arrangements entered into by State/Territory entities that are universities are non-core arrangements under the Act. The Act details the obligations for a State/Territory entity to notify the Minister when proposing to enter a non-core arrangement and upon entering the arrangement, the Minister's powers to make a declaration in relation to an arrangement and consequences for contravention of a declaration.

GLOSSARY

Academic freedom

University staff and students can engage in intellectual inquiry, express their opinions and beliefs and contribute to public debate free from intimidation, harassment and censorship, consistent with the definition of academic freedom provided in the *Higher Education Support Act 2003 (Cth)*.

Accountable authority

An accountable authority is a senior executive or executive body, responsible and accountable for the security of people, information and assets to counter foreign interference.

Cybersecurity

Cybersecurity refers to the technical and people capabilities, leadership, culture, techniques and practices that collectively protect an organisation's digital infrastructure and safeguard its data, systems and business operations against unauthorised access, attack, manipulation, disruption or damage.

These threats may come from an adversary, a malicious or careless insider or through lack of investment in the safety of systems or infrastructure.

Declaration of interest disclosure

The process of disclosing any interests that could constitute a real, potential or apparent conflict of interest.

Due diligence

A process where all reasonable steps are taken to obtain relevant information that will help reduce the risk of making an uninformed decision.

Espionage

Espionage is the theft of Australian information by someone either acting on behalf of a foreign power, or intending to provide information to a foreign power that is seeking advantage.

Foreign influence

All governments, including Australia's, try to influence deliberations on issues of importance to them. These activities, when conducted in an open and transparent manner, are a normal aspect of international relations and diplomacy and can contribute positively to public debate.

Foreign interference

Foreign interference occurs when activities are carried out by, or on behalf of, a foreign actor that are coercive, clandestine, deceptive or corrupting and are contrary to Australia's sovereignty, values and national interests.

Internet of Things

A catch-all term for the growing number of electronic devices that are not traditional computing devices but are connected to the internet to send data, receive instructions or both.

Positive security culture

A positive security culture gives people confidence that they can speak openly about security-relevant incidents and will see the organisation improving as a result, and confidence that any actions or decisions will be reviewed fairly. This allows people to focus on what is best for the organisation, rather than on protecting themselves.

Resilience

The capacity of universities to deter, withstand and recover rapidly from acts of foreign interference.

Self-censorship

The act of intentionally and voluntarily suppressing information from others when formal impediments are absent.

Staff and students

Used throughout the text to refer to members of the university community.

Threat modelling

Threat modelling is the proactive process of identifying potential risks and threats, then creating tests and countermeasures to respond to potential threats. Threat modelling for cybersecurity is a rapidly evolving discipline: threat models can be created for almost any imagined scenario.

Successful threat modelling involves identifying potential threats, analysing the possible effects of those threats, determining whether the threat is significant and whether it requires a neutralisation strategy.