Charles Sturt University

UNIVERSITY FOREIGN INTEFERENCE STEERING GROUP

University Foreign Interference Taskforce-Input into Draft Guidelines

29 October 2019

Office of the Vice-Chancellor
Charles Sturt University

Charles Sturt University

Office of the Vice-Chancellor

29 October 2019

Mr Cameron Ashe
Chair - University Foreign Interference Steering Group
Acting National Counter Foreign Interference Coordinator
Department of Home Affairs
6 Chan Street
BELCONNEN ACT 2617

Dear Mr Ashe

UNIVERSITY FOREIGN INTERFERENCE TASKFORCE – INPUT INTO DRAFT GUIDELINES

On behalf of Charles Sturt University, I am pleased to provide this response to the University Foreign Interference Taskforce's call for input into the *Guidelines to Counter Foreign Interference in the University Sector - University Foreign Interference Taskforce,* of October 2019. Our response has been prepared based on the structure of the Guidelines, a copy of which is provided for reference at Attachment A.

Charles Sturt University is Australia's largest regional university, with more than 43,000 students and approximately 2,000 full time equivalent staff. We are a unique multi-campus institution with campuses at Albury-Wodonga, Bathurst, Canberra, Dubbo, Goulburn, Manly, Orange, Parramatta, Port Macquarie and Wagga Wagga, as well as various study hubs located in regional south-eastern Australia.

Our regional focus is complemented by our teaching and learning offerings at study centres in each of Brisbane, Melbourne and Sydney. While the University has a small number of international students studying at our regional campuses, most of the University's international student load attends our metropolitan centres. Currently, the University's top five markets for international students are India, Nepal, Sri Lanka, China and Bangladesh. Further, the University maintains partnership agreements in many countries including China, Cambodia and India.

While the University undertakes market and operational activities in a wide range of countries with differing systems of government and alternative models of society to ours, Charles Sturt University believes that western values and liberal institutions provide the fundamental foundations for economic prosperity, social inclusion and environmental sustainability. Protecting our public institutions from foreign interference is vital to ensure that our way of life is not only continued, but is strengthened, in an ever-changing world. This is why, in previous submissions the University has supported the bipartisan efforts of the Parliament and the initiatives of the Government to inhibit foreign interference.

Charles Sturt University supports the Taskforce's approach to the development of the Guidelines, including the four strategic areas – culture and communication, foreign collaboration, research and intellectual property and cyber security on which the Guidelines are structured. Building on these areas, the University also supports the objective of the Guidelines, which is to provide additional guidance on which universities can draw to assess risk in their global engagements, and to safeguard their people and data.

In addition, Charles Sturt University recognises that the Taskforce has developed the Guidelines based on the foundational principle of university autonomy. Whereby, flexibility in how each university will draw on the

Guidelines and associated resources can be tailored and customised to the unique business circumstances of each institution. Further, we welcome the Taskforce's approach that the Guidelines have been developed and prepared to inform each university's existing protocols and protections. We suggest that the Taskforce strengthen the communication of this thinking in the documentation associated with the Guidelines. Regarding the elements of the Guidelines themselves Charles Sturt University provides the following commentary and suggestions.

Culture and Communication

Charles Sturt University agrees that institutional culture and organisational communication should be the primary strategy and first line of defence for countering the potential for foreign interference. An appropriate level of awareness and maintenance of culture of alertness is critical to avoiding foreign interference in a university's business and is consequently in the national interest. It is also crucial to maintain an institution's reputation in the marketplace and the institution's underlying financial viability.

Embedding a culture of alertness within universities, can readily be achieved by reviewing policies, structures, frameworks and communication strategies to ensure that they promote and strengthen a culture of safety and security, and resilience to foreign interference. To this end, strengthening a culture of alertness can most effectively be achieved incrementally by building on existing organisational arrangements.

Charles Sturt University believes that this opportunity could be further highlighted in the Guidelines to ensure rapid uptake of the practices put forward in the Guidelines. Further, the University also suggests that the Department could provide a range of tools and templates for addressing foreign interference to assist universities with the revision of policies, structures, frameworks and communication strategies.

Charles Sturt University agrees that the key institutional strategies to ensure foreign interference in an institution's governance, management and operations does not occur include:

1. Accountable Authorities.
2. Foreign Interference Risk Planning.
3. Communication and Education on Foreign Interference Risks.
4. Regular Evaluation and Review of Foreign Interference Risk Planning and Mitigation for Robust Quality Assurance.

Foreign Collaboration

Ensuring university international collaborations are entered into and undertaken in Australia's national interest is a crucial strategy and line of defence for countering the potential for foreign interference. Building on the culture and communication elements discussed above, the nature and purpose of collaboration with international entities must be transparent, undertaken with full knowledge and consent, and in a manner that avoids harm to Australia's interests. To be successful these considerations must provide the basis from which the appropriate level of awareness and the maintenance of a culture of alertness is built within an institution.

Charles Sturt University supports the Taskforce’s position that the key institutional strategies to ensure foreign interference in an institution’s international collaborations does not occur include:

1. Knowing international partners.

2. Ensuring good governance, however, we do believe that the Guidelines could be strengthened to include professional management within this strategy.

3. Transparency and knowledge sharing.

Like Charles Sturt University, most institutions with foreign collaborations have extensive due diligence policies and procedures and service level agreement arrangements that ensure partner knowledge, governance and management and transparency are maintained. There is always the opportunity to improve policy and procedure in this space. The Guidelines could be refined to make this connection.

Research and Intellectual Property

Charles Sturt University agrees that research is a powerful driver of growth in modern economies, indeed we note that successive Commonwealth and State governments in Australia have actively promoted and encouraged universities to enter into international collaborations and undertake cross-border research activities over the last few decades.

Charles Sturt University notes that an objective of the Guidelines is to support educative and policy responses for Australian researchers that participate in the international research system to ensure research and research training integrity. Enabling the research community to recognise and respond to these growing trends while maintaining the openness that underlies the success of our research sector will be vital to guard against foreign interference while protecting the intentional reputation of Australia’s universities. The University also recognises that efforts to protect against foreign interference are likely to enhance the perceived value of Australian research to foreign governments and that in turn such efforts may actually lead to an increase in attempts to compromise the integrity of the research system.

Charles Sturt University agrees with the Taskforce that it is important that the contribution that university generated research and intellectual property makes to the economic, social and cultural advancement of the nation is protected. Including guarding against threats such as foreign interference, including diversions that seek to suppress academic activity, attempts to misappropriate research or direct research in a clandestine way. To this end, the University supports the strategies put forward in the Guidelines aimed at ensuring foreign interference and international theft of research and intellectual property does not occur including:

1. Proactive proportionate approach to risk, however the University believes that this strategy could be strengthened by the development and provision of tools by the Department for universities that takes into account the national interest (which, in itself may not necessarily be obvious or known to institutions themselves).

2. Know university research staff and collaborators, this section of the Guidelines could be strengthened by highlighting the human cultural and capital elements of this strategy.

3. Consider potential end-use possibilities, again this strategy could be strengthened by the development and provision of tools by the Department for universities that takes into account the national interest.

Cyber Security

The frequency and sophistication of attacks to thwart unauthorised access, manipulation, disruption or damage, and ensure the confidentiality, integrity and availability of information of institutional information systems is ever increasing. The University notes that the Guidelines have been developed to assist universities to manage and protect their networks, as well as detect and respond to cyber security incidents should they occur. The University also supports and agrees with the strategies put forward to address foreign cyber-attacks in the Guidelines, including:

1. Implementation of university cyber security strategies.

2. Cyber-intelligence sharing across the sector and with Government.

3. Cyber security as a whole-of-organisation “human” issue, with strong emphasis on a positive security culture.

4. Cyber threat-models to understand and mitigate business risks.

Charles Sturt University believes that the Guidelines could be strengthened so that strategies aimed at defeating foreign cyber-attacks are considered in university quality assurance and risk management frameworks, as well as continuous improvement policy and procedure. Further, development and implementation of university cyber security strategies could be strengthened by building on the knowledge and resources of the Department in this area of highly specialised expertise. The Taskforce may provide an appropriate mechanism to maintain and build this function on a collaborative basis between the university sector and the Department.

In conclusion, Charles Sturt University recognises that a careful balance must be struck between protecting the national interest and not placing unnecessary burden on the sector. The University believes that the Guidelines have effectively struck this balance. We believe that the approach set out in the Guidelines meets the shared objective of both universities and the Government to safeguard the security of Australia’s university sector without undermining the invaluable asset of its openness, which optimises benefits to our community.

Finally, Charles Sturt University supports the approach adopted by the Government that the Guidelines are not intended to place additional compliance or regulatory burdens on universities and that neither are they intended to be exhaustive of all considerations by universities about foreign interference risks. The University supports the Guidelines and believes that they will support universities to examine existing tools, assist decision makers to assess the risks from foreign interference and promote greater consistency across the sector.

I would be very pleased to provide further information to the Taskforce and would be available to provide evidence at any proposed consultations that that Taskforce may undertake in relation to ensuring Australia’s western values and liberal institutions are protected from foreign interference.

Yours sincerely

Andrew Vann

Professor Andrew Vann
Vice-Chancellor

Attachment A:

Guidelines to counter foreign interference in the university sector

University Foreign Interference Taskforce

DRAFT

Contents

DRAFT

Guidelines to counter foreign interference in the university sector

University Foreign Interference Taskforce

Context Statement

A defining factor in the world-class performance and reputation of Australia's university system is its openness to the world. The globally engaged nature of our universities is indispensable to their success. Indeed, it is the bedrock of their competitiveness.

This global engagement enables Australia to make cutting-edge research breakthroughs as our own world-class academics work in collaboration with others worldwide at the forefront of their field. It enables us to educate many of the world's best students, who return home after graduation with an enduring knowledge of, and lifelong affection for Australia - a powerful soft power asset for the nation. It enables Australia to recruit outstanding global experts to teach and conduct research in our universities, catapulting our capacity ahead of our competitors. And it ensures the learning and the alumni networks of Australian university students are enriched by classmates from all around the world. International experience and collaboration is integral to the academic career path around the world. A global exchange of ideas is enabled by this exchange of people.

The Australian Government supports such international collaborations through its programs and policy settings across a wide range of initiatives and portfolios. These include appropriate visa settings and the new Global Talent visa; a comprehensive program of Australian Trade Commission work to promote international education; the New Colombo Plan; the eligibility of international academics for several Australian National Competitive Grant schemes; the provision of targeted research funds such as the Australia-China Science and Research Fund and the Australia-India Strategic Research Fund; and providing support for Australian students and academic staff to travel internationally.

This crucial global engagement occurs in an ever more complex world. New challenges and threats are evolving globally, including to intellectual property and IT systems. The recent cyberattack on the Australian National University (ANU) is a high-profile example of these threats. For decades, Australia's universities have had strong working relationships with government agencies on security matters, and have regularly sought advice to help safeguard their people, research, systems and intellectual property, as well as rebuff attempts to breach security. Universities and government know that a robust and trusted system of international collaborations is one in which risks are managed and benefits realised.

Our nation's universities and government established a joint taskforce to enhance these existing safeguards against foreign interference. In a world of more complex risks, we are working together to add to the current protections, while preserving the openness and collaboration crucial to the success of Australia's world-class university system. This work is guided with equal input from the university sector and government agencies. It draws on the expertise of our universities in nurturing this vital global engagement, and on the insights of our security agencies into emerging threats.

DRAFT

The taskforce focused on four strategic areas – culture and communication; foreign collaboration; research and intellectual property; and cyber security.

The objective is to provide additional guidance on which universities can draw to assess risk in their global engagements, and to safeguard their people and data. Crucially, too, this work upholds the foundational principle of university autonomy – preserving flexibility in how each university might draw on these resources. These guidelines further inform each university's existing protocols and protections.

There is a careful balance to be struck. 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.

These guidelines are not intended to place additional compliance or regulatory burdens on universities neither are they intended to be exhaustive of all considerations by universities about foreign interference risks.

The purpose of these guidelines is to support universities to examine existing tools, assist decision makers to assess the risks from foreign interference and promote greater consistency across the sector.

DRAFT

The threat environment

In September 2019, Australia's then Director-General of Security, Mr Duncan Lewis, noted the current scale of foreign interference activity against Australia's interests is unprecedented.[1] In some cases, foreign actors are pursuing opportunities to interfere with Australian decision makers across a range of sectors in Australian society – including the university and research sectors.

An appropriate response to the threat of foreign interference by the university sector 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 Counter Foreign Interference (CFI) Strategy, which aims to increase the cost and reduce the benefit to foreign governments of conducting foreign interference in Australia.

Foreign actors can use a range of coercive, clandestine, corrupting and deceptive means to achieve their aims in the university sector. These may include:

- academic collaboration;
- economic pressure;
- solicitation and recruitment of post-doctoral researchers and academic staff;and
- cyber intrusions.

[1] ASIO, Director General's Review, https://www.asio.gov.au/AR2018-01.html

Introduction to the guidelines

Upholding the foundational principle of university autonomy, some key themes guide this work to deepen resilience against foreign interference. These include:

Promote and strengthen a positive safety and security culture
Promote and strengthen a culture of safety and security, and resilience to foreign interference. Deepening and enhancing a safety and security culture supports an environment of trust and confidence in a consistent manner across the university sector that guides decision making, based on potential risks.

Communication and education about foreign interference risk
The development of additional communication strategies and education programs to raise awareness of foreign interference risks. Communication strategies, education and professional development programs promote the university's commitment to safety and security culture, and raise awareness of risks and their implications.

Risk Planning
Including foreign interference risks in risk frameworks, policies and procedures promotes a strong security culture and avoids unnecessary duplication. Universities already have policies, frameworks, systems and processes to ensure a positive security and safety culture, enabled by robust communication, and due diligence. This includes identifying capabilities in the university that contribute to the security of people, information and assets.

Due Diligence
Know your partner, research collaborators and staff by undertaking appropriate due diligence, supported by university processes, which takes account of the profile of foreign interference risks. Much international collaboration involving Australian universities consists of informal partnerships, such as dialogue and co-operation between individual staff. These partnerships involve the exercise of core values such as freedom of enquiry. This is to be supported. Academics and other employees of Australian universities also have a responsibility to act ethically and in good faith and university processes that inform staff about foreign interference risks can help them to do so.

Knowledge sharing across the sector and with the Commonwealth
Strengthen knowledge sharing mechanisms across the sector and between the sector and the Commonwealth, about emerging risks and experiences of foreign interference. Universities have mechanisms to raise awareness of emerging threats and experiences by sharing examples among the sector. This includes sharing examples of foreign interference, attempts to exert undue influence, or otherwise undermine academic freedoms and values.

DRAFT

Scope of the guidelines

These guidelines may be used to guide university activities and initiatives to minimise the risk of foreign interference. Universities already have policies, frameworks, systems and processes in place to ensure a positive safety and security culture. The purpose of these guidelines is to emphasise educative and policy responses to assist decision makers to assess the risks from foreign interference and promote greater consistency in risk mitigation strategies across the sector.

These guidelines are informed from international experience and draw upon risk management policies, and safety and security practices already implemented by Australian universities.

These guidelines:

- are intended to **support an environment of trust and confidence** in a consistent manner across the university sector to guide decision-making based on potentialrisks;
- are **supported by a range of questions that universities can use** to satisfy themselves they are addressing the range of emerging risks in global higher education arising from foreign interference;
- checklists provided are aimed to **equip institutions and individual staff members to enhance a positive safety and security culture** to help safeguard against foreign interference;
- prioritisation guidance is intended to support decision makers **balance priorities** and acknowledge the different capability and maturity levels across the sector; and
- **are not intended to place additional compliance or regulatory burdens** on universities neither are they intended to be exhaustive of all considerations by universities about foreign interference risks.

DRAFT

Strategic areas
Culture and Communication

1.0 Objective

Universities have policies, structures, frameworks and communication strategies to promote and strengthen a culture of safety and security, and resilience to foreign interference.

1.1 Accountable Authorities

A senior executive responsible and accountable for the security of people, information and assets strengthens resilience to foreign interference.

I. Accountable authorities oversee security and safety risks and are responsible for risk mitigation strategies

An accountable authority oversees the ongoing development and review of policies, structures, and frameworks to assess, monitor, and mitigate the risks of foreign interference, and the development of a positive safety and security culture to foster individual responsibility to manage such risks.

Key considerations

- Who in your university has operational responsibility for foreign interference and safeguards?
- What practices and processes promote awareness of safety and security to safeguard against foreign interference?
- Who in your university has senior executive responsibility for foreign interference and safeguards?
- What processes does your university have that trigger engagement with relevant Commonwealth agencies on legislative compliance and foreigninterference?

Checklist

An accountable authority has responsibility and accountability for:

- the security of people, information and assets to counter foreigninterference;
- overseeing the university's risk reporting framework to reflect its safety and security strategy and detail how it is addressing areas of vulnerability and associated risks, including foreign interference; and
- reporting to the university governing body in accordance with existing risk frameworks, reporting arrangements, review and evaluation.

DRAFT

II. A Chief Safety and Security Officer (CSSO) or other senior executive tasked as a CSSO

Checklist

A CSSO or other senior executive oversees work to safeguard against foreign interference including:

- liaising between the university and government agencies onsecurity;
- supporting the accountable authority in the university to ensure the safety of people (including staff, students, contractors, visitors and clients), informationandassets;
- embedding safety and security management awareness and risk mitigation practices to guard against foreign interference;
- overseeing information safety and security awareness training programs for staff and students including those located or travelling overseas;
- in conjunction with the relevant area (e.g. IT, HR), managing the university's response to safety and security-related incidents, in accordance with the institution's security incident and investigation procedures, and overseeing monitoring mechanisms across the entity to guard against foreign interference;
- monitoring procedures to achieve required protections, address risks, counter unacceptable safety and security risks, and improve security maturity; and
- disseminating and managing intelligence and threat information to stakeholders across the university, informed by advice from staff and governmentagencies.

Note: The scope and complexity of the CSSO role depends on the nature of the university’s business and its risk environment. For instance, universities may have an Audit and Risk committee for which this role may be relevant. For some universities, the accountable authority may take on the role of the CSSO and delegate the day-to-day functions of protective security as appropriate.

1.2 Foreign Interference Risk Planning

I. Universities incorporate into existing relevant frameworks foreign interference threats and vulnerabilities to the university’s people, information and assets and outline mitigation measures

Integrating foreign interference risks in existing risk frameworks, policies and procedures promotes a strong security culture and avoids unnecessary duplication.

Universities already have policies, frameworks, systems and processes to ensure a positive security and safety culture, enabled by robust communication, and due diligence. This includes identifying capabilities in the university that contribute to the security of people, information and assets.

Consistent internal reporting mechanisms enable the sharing of security reporting with government agencies to enhance understanding of the security environment in universities.

Key considerations

- How do policies and procedures acknowledge foreign interference as a risk?
- How do policies and procedures enable staff and students to understand who is affected by specific security risks?
- How have all stakeholders been considered in safety and security policies andprocedures?
- What processes manage responses to security incidents?
- What is the escalation pathway and how is the appropriate response to these risks clearly articulated?
- How consistent are internal reporting mechanisms to support internal evaluation and communication with external stakeholders?
- How clear are roles and responsibilities across the university about when to engage with Commonwealth agencies to ensure compliance with Defence Export Controls, the Foreign Influence Transparency Scheme and Autonomous Sanctions?
- How is the level of risk involved in a particular research project, and the nature of the governance and oversight that could be applied to mitigate this riskconsidered?
- What documentation captures these considerations, and can be referred to, should a retrospective assessment of the research activity beundertaken?

Checklist

- Clear mechanisms for staff and students to report foreign interference with oversightby the CSSO or equivalent.

- Regular review of processes, guidance and communications for the security of people, information and assets for overseas travel with the risk of foreign interference inmind.

- Fully integrated protectivesecurity in planning, selecting, designing and modifying facilities for the protection of people, information and physicalassets.

- Robust processes to remove systems access for university staff and studentsafter they leave the institution with the risk of foreign interference inmind.

- Physical security measures that minimise or remove the riskof:
  - harm to people, and
  - information and physical assets being rendered inoperable or inaccessible, or being accessed, used or removed withoutauthorisation.

DRAFT

DRAFT

1.3 Communication and Education on Foreign Interference Risks

I. University communication plans and education programs raise awareness of foreign interference risks

Communication plans and education programs enhance a robust security culture and awareness of foreign interference risks.

Key considerations

- What training does your university provide to promote awareness of foreign interference risks?
- What communications and protocols support staff and students to follow reporting requirements on foreign interference?

Checklist

- A communication strategy promotes the university's commitment to safety and security culture, and raises awareness of the risk and itsimplications.
- Education and professional development programs seen as opportunities tointegrate awareness on foreign interference risk andmitigation.
- Integrated capabilities in university positions thatcontribute to the safety of people, information, and assets to safeguard against foreigninterference.

1.4 Regular Evaluation and Review of Foreign Interference Risk Planning and Mitigation for Robust Quality Assurance

I. Universities regularly assess the maturity of their safety and security strategy, policies and procedures as they relate to foreign interference, and incorporate into risk reporting cycles

Checklist

- Regularly assess the maturity of risk planning and mitigation under the university's safety and security strategy, policies and procedures on foreigninterference.
- A mechanism to promote best practice and lessons learned as a cycle of action, drawingon evaluation and learning.
- Regularly review communication plans and education programs on foreign interference.

Foreign Collaboration

2.0 Objective

The nature and purpose of collaboration with international entities is transparent, undertaken with full knowledge and consent, and in a manner that avoids harm to Australia's interests.

2.1 Know your partner

Universities need to know their partners by undertaking appropriate due diligence informed by knowledge of foreign interference risks.

I. Staff are supported by university processes that assist them to be mindful of foreign interference risks when collaborating with an internationalpartner

Much international collaboration involving Australian universities consists of informal partnerships, such as dialogue and co-operation between individual staff. These partnerships involve the exercise of core values such as freedom of enquiry. This is to be supported. Academics and other employees of Australian universities also have a responsibility to act ethically and in good faith and university processes that inform staff about foreign interference risks can help them to do so.

Key considerations

- What processes ensure staff are aware of foreign interference risks, even in informal collaboration and communication?
- What guidelines support staff and student understanding of these processes where appropriate?
- How are academic staff, professional staff and research students, required to undertake training in recognising foreign interference risks in everyday work, communications and international travel?
- What level of senior executive oversight exists for internationaltravel?

II. Before entering into a formal partnership agreement, due diligence is completed to establish who the partner is

International collaboration in Australian universities can involve formal arrangements with partner entities such as another university or company. Due diligence includes inquiry into the partner's past activities, the sectors it operates in or is associated with, the beneficial owners and the commercial and ethical standing of its governing body.

Key considerations

- To the extent that it is reasonable for a university to determine, do partners or their associates have relevant research backgrounds, is their organisation reputable, and are reasonable background checks conducted for new people working on aproject?
- What elements of the activity need to be scoped differently as a result of the partnership and if so, do the benefits outweigh the risks?

DRAFT

III. Institutional risk management frameworks are cognisant and responsive to activities covered by federal and state legislation, regulations and codes ofconduct

In any partnership, the foreign interference risks depend - to a significant extent - on the collaborative activity being proposed. Some activities are covered by specific legislation, regulation and codes of conduct such as the *Defence Trade Controls Act 2012* (DTCA) and Autonomous Sanctions legislation.

Key considerations

- How does the partnership consider potential internal and external risks to the university where it may be appropriate to obtain executive advice andapproval?
- Does the partner or the backing entity appear on any public registers (Foreign Influence Transparency Scheme, Register of Lobbyists, Grants Register (GrantConnect) and – to the extent that it is reasonable for the university to be able to determine – is the partner being upfront and transparent about their affiliations, parent partners and intent?
- Does the research activity proposed involve items or goods listed on the Defence Strategic Goods List? Are the proposed research activities captured by the Defence Trade Controls Act?

IV. For collaborations that continue over an extended period, due diligence assessments of partners are revisited and formal agreements are subject to regularreview

Risks from foreign interference stemming from collaborative activities can evolve over time as partners themselves or external circumstances change.

Key considerations

To the extent that it is reasonable for universities to determine:

- Have collaborators' behaviours and interests changed over time into something which the university or individual is not comfortable with?
- What mechanisms support staff to identify foreign interference risks from collaborative partners who are undertaking extended stays, do not have the appropriate background, or engage in unusual activity?

DRAFT

Checklist

- Conduct due diligence activities to help check that the proposed activities comply with the university's policies on academic freedom; audit and risk; and research ethics andintegrity.
- Conduct due diligence reviews and regular risk assurance updates.
- Collaborations with foreign partners involving research in particularly sensitive areas are subject to more due diligence arrangements.
- If due diligence investigations raise concerns, processes to guide the university to review the ethical, security, legal and reputational risksinvolved.
- Provide senior executive with visibility of international travel, to assist in due diligence of risk while staff are overseas.
- Ensure there is a clear point of contact to seek advice or support forengagementactivities.

2.2 Good Governance

Agreements with international partners comply with Australian law and address potential threats to the integrity of the research and reputation of the university and identify emerging or potential risks, including any foreign interference and security risks.

I. When formally engaging international organisations or individuals in collaborations, contracts, partnerships or alliances, a university undertakes due diligence on the intended partner and the areas of collaborations are explicitlyarticulated

For all formal interactions with foreign institutions or individuals, best practice contracting mechanisms and policies should reduce the risk of foreign interference. Terms and conditions of agreements or Memoranda of Understanding (MoUs) should include clauses that protect the integrity of the activity. Internal stakeholders including operational and academic staff benefit from having access, through internal training and awareness sessions, to simple risk assessment tools to manage foreign engagement including visits and foreign delegations. The tools assist to improve academic research and teaching integrity. This is good practice for any engagement with external bodies, not only with foreign entities.

Key considerations

- What background is known about the university's partner and is there anything dubious about their interests being reported?
- How upfront and transparent is the partner being about affiliations, parent partners and intent, that it is reasonable for the university to be able to identify? These may include existing vendor relationships, sourcing partners and alliances with interest in the primarypartner
- How are contracts drafted to give the university clear authority to withdraw from the agreement should the partnership impinge on academic freedom and research ethics or be found to be subject to export controls?

DRAFT

Checklist

- Consider foreign collaboration and ethical, security and reputational risks as an important, regular agenda item for meetings of senior staff.
- Visibility of collaboration agreements for senior executives, which streamlines governance, oversight, due diligence and riskassessment.

<u>Central registry</u>

- Senior university executives need visibility of all formal collaboration agreements. A central registry (or similar) of international collaboration agreements brings consistency and oversight to such engagements, and streamlines governance, due diligence and risk assessment.

<u>Contract management</u>

- Consideration should be given to whether or not an arrangement is to be legallybinding or non-binding such as an MoU, International Cooperation Agreement or other form of contract.
- Agreements with foreign partners:
    - Should affirm the primacy of Australian law and the university's written policies over the law of the foreign partner institution, for all relevant activities taking place in Australia.

<u>Review</u>

- Universities review agreements annually including to assess new risks andpotential vulnerabilities that may have emerged during an internationalcollaboration.
- Internal training and awareness sessions help manage international engagement including visits and foreign delegations.

II. University policies and procedures that outline the requirements for staff, students, contractors and honorary staff engaging in internationalcollaboration

Roles, responsibilities and accountabilities for all levels of management in international collaborations are clear to all internal stakeholders. Policies and procedures are written in clear language and are simple to implement. Policies cover practical measures to mitigate risks in foreign interference, protect the core values of the institution, and provide guidance to support compliance with the DTCA and other regulations.

DRAFT

Key considerations

- What level of visibility do senior administrators and officials in universities have of staff appointments?
- What processes ensure staff are aware of their rights and obligations at the university?
- What training does the university offer to staff to build capacity in identifying potential instances of foreign interference?
- What mechanisms assist staff to identify and mitigate possiblerisks?

Checklist

- Senior executive oversight of staff appointments, including secondary titleholders (e.g., honorary and adjunct appointments).

- Templates to guide staff considering international collaboration, including due diligence checklists to guide researchers who plan to enter into formal collaboration agreements with foreign partners.
    - These may include prompts to mitigate potential risks, protect core values such as academic freedom and free speech and ensure compliance with export control laws and other regulations.

- Policies and processes for staff to report issues or to discussconcerns.

- Awareness among staff of possible actions by foreign institutions that may be inconsistent with Australia’s academic freedoms and values and the university’s interests. These may include:
    - Demands – or inducements – to change content in subjects driven by a foreign political, religious or social agenda.
    - Demands – or inducements – to cancel visits or activities where the visits or activities are considered at odds with a foreign political, religious or socialagenda.
    - Demands – or inducements – to grant unnecessarily broad access to the university’s information systems.
    - Use of acquired access to provide access to unapproved thirdparties.
    - Monitoring of academic staff, administrators, students or visitors to gauge their positions on topics considered sensitive by foreign interests.
    - Harassment, hostility, intimidation or other negative conduct toward academic staff, administrators, students or visitors seen to hold positions on issues at odds with a foreign political, religious or social agenda.
    - Intrusion into life on campus for purposes of coercing and ‘policing’ a student population, particularly with a view to suppress criticism ordissent.
    - Presence of unfamiliar individuals at lectures or other activities on topics considered sensitive by foreign interests.

- If staff members become aware of such activities (including online through social media or other forums) these should be reported to the Chief Safety and Security Officer or relevant senior line manager. These matters may then be raised with government agencies.

DRAFT

2.3 Transparency and Knowledge sharing

Universities have mechanisms to raise awareness of emerging threats and experiences by sharing examples among the sector. This may include examples of interference, attempts to exert undue influence or otherwise undermine academic freedoms and values.

I. Universities build a repository of information on interference-associated foreign collaboration which can be shared internally

Government agencies may be able to help universities identify instances, or attempts, of foreign interference. Additionally, universities are well placed to detect whether undue influence may be being exerted on their campuses. Universities should endeavour to establish a reporting mechanism, or designated officer, to liaise with government to establish a two-way avenue of communication about risks.

Key considerations

- How do staff have ready access to information on potential partners that have engaged with the university in the past?
- How are responses to Freedom of Information requests on international collaboration made available to relevant staff in the university?

II. Interference-associated foreign collaboration risks that could have adverse impact broader than one university are shared across the higher educationsector

Where there is a risk that could affect the broader sector, institutions should consider sharing knowledge and risk mitigation opportunities with other sector partners where appropriate. Information regarding partnerships or identified instances of interference and undue influence can be helpful to other institutions.

Key considerations

- How are experiences shared to help others and what opportunities are there to provide feedback and share lessons learned?
- What is the shared point of contact at universities for collaboration and information sharing across the sector?

III. When a new interference-associated foreign collaboration risk is identified, the knowledge is shared with relevant government agencies

Government agencies may be able to help universities identify threats of foreign interference so appropriate reporting of threats and occurrences of foreign interference is important. Universities report all threats and occurrences of foreign interference. Liaison between universities and government agencies on security is typically done by an existing designated member of the executive team.

DRAFT

Key considerations

- How do staff understand what risks should be shared with governmentagencies?
- How do staff know who their university contact is for liaison with governmentagencies?

IV. Universities provide staff with access to channels which reports threats of foreign interference to their university and the broader higher educationsector

It is important for staff to be aware of new and on-going threats to the university. Where instances of foreign interference have occurred or been attempted, and where it is deemed beneficial to do so, universities consider reporting more broadly to staff and the sector current threats and risk mitigation opportunities.

Key considerations

- How does existing guidance to staff outline best practice on transparency of international relationships and affiliations between individuals and universities?

V. Universities have a Conflict of Interest (CoI) policy which identifies foreign affiliations, relationships and financial commitments that set out staff responsibilities to their Australian university

Universities may include reporting requirements in their existing CoI agreements to identify staff who have international financial interests, including affiliations with international institutions.

Key considerations

- How do the university's CoI procedures include international financial and otherinterests?
- How do the university's CoI procedures include secondary staff employment, such as honorary and adjunct staff?
- What processes monitor how conflicts are treated and reported? These may include prompts to mitigate potential risks, protect academic freedom and free speech, and ensure compliance with export control laws and other regulations.

DRAFT

Checklist

- Should a university believe it has been subject to foreign interference or come under significant undue influence by a foreign partner, it registers its concern withASIO.

- Provide appropriate, internal reporting of funding sources to help avoid reputational damage and better manage perception of undue influence orinterference.

- Procedures ensure donations from international companies or Australian-based companies with strong foreign links are consistent with the university's policies and place no undue influence on the academic program.

- The university's policies include advice on international travel, staffing appointments and engagements, and bribery, corruption, foreign donations andgifts.
  - The Australian government Department of Foreign Affairs and Trade provides regularly updated travel advice for individual countries. www.smartraveller.gov.au
  - Anti-Bribery & Corruption (ABC) A guide for Australians doing business offshore. https://www.austrade.gov.au/

- Universities can access advice from the Australian Security Intelligence Organisation's (ASIO) *Business and Government Liaison Unit* (BGLU), which provides security advice to Australian businesses.
  - The BGLU liaises between ASIO, government, industry, and academic stakeholders. The BGLU provides information including via a subscriber-controlled website, ASIO-hosted briefings, face-to-face engagement andforums.
  - The BGLU website operates on a free subscription basis. It has intelligence-backed reporting and resources. To subscribe: https://www.bglu.asio.gov.au/

DRAFT

Research and Intellectual Property (IP)

3.0 Objective

Research is a powerful driver of growth in modern economies. This enhances its perceived value to foreign governments. Attempts may be made to compromise the integrity of the research system. The primary objective of these guidelines is to support educative and policy responses for Australian researchers to participate in an international research system that has integrity by enabling our research community to recognise and respond to these growing trends while maintaining the openness that underlies the success of our research sector.

It is important that the contribution that university generated research and intellectual property makes to the economic, social and cultural advancement of the nation is protected. This includes guarding against threats such as foreign interference, including diversions that seek to suppress academic activity, attempts to misappropriate research or direct research in a clandestine way.

3.1 Proactive proportionate approach to risk

Effective research processes are built on collaborations, partnerships and engagement between researchers, end users (those who use or benefit from research) and other stakeholders. These guidelines aim to identify the actions necessary to ensure the maintenance of an environment where research is inherently enabled by effective management.

I. Researchers, professional staff and Higher Degree Research (HDR) students areaware of the ways in which foreign interference canoccur

The nature of research offers multiple entry points for potential foreign interference. Universities should provide training to staff and HDR students on how foreign interference activities may manifest and provide information on the supports in place should they become of aware of foreign interference.

Researchers should consider the intentional and unintentional potential consequences if foreign interference occurs. Key questions include:

- Who might be affected by this research – positive and negativeconsequences?
- How might they be affected?
- What might be affected by this research – positive and negativeconsequences?

University guidelines and advice could adapt existing security and personal safety protections as required.

Key considerations

- What training currently exists? How is it appropriately targeted to provide information about the more subtle forms of foreign interference?
- How can current university guidelines, for example human ethics, safe travel arrangements, facility access and event management, continue to be enhanced to identify potential risks and support researchers in high risk or sensitive research areas to proactively managetheirrisks?

DRAFT

II. Clear university risk assessment and reporting frameworks

Core to the management of foreign interference is the identification and management of risk. Universities should take a risk-based management approach to minimise the impact of foreign interference on their informal and formal research activities and any intellectual property it creates. The aim of a risk-based approach is to determine:

- in *prospect*, the level of risk involved in a particular research project, and the nature of the governance and oversight that could be applied to mitigate this risk,and
- regardless of the decision, ensure documentation of the considerations, which can be used should retrospective assessment of the research activity beundertaken.

Noting that there may be a very different perspective of the potential risk before and after an event has occurred.

Further information about risk planning is found at section 1.2 Foreign Interference Risk Planning.

Key considerations

- How robust are your risk framework mitigation strategies that deal with foreign interference in research?
- Who is responsible for maintaining, promoting and applying thesearrangements?
- How are these arrangements informed by the range of research undertaken in the university and the associated level of risks?

III. Transparent and robust reporting requirements be developed, documented and maintained

Those seeking to interfere with, or influence, Australia's research effort may attempt to alter or direct the research agenda into particular areas of research. This can occur through subtle forms of influence and engagement and through funding arrangements that may lead to loss of future value and/or control of intellectual property.

At the organisation level, internal reporting of international contacts (or at least international collaborative partners) in research and potentially as donors helps to builds the capacity for early awareness and transparency among the university's stakeholders.

Key considerations

- What ability and capacity does the university have to analyse and respond to the information gathered from internal reporting arrangements?
- What level of executive oversight exists for staff appointments, including secondary appointments (e.g. honorary and adjunct roles)?
- What minimum level of due diligence are foreign investments and partnerships at all levels subject to?
- What level of internal reporting is in place for foreign investments and partnerships and does this aid accountability and risk management?

DRAFT

Checklist

- Risk management plans and reporting frameworks appropriate for the types of risks faced by each university are developed and maintained.
- Researcher training in foreign interference is delivered. This could include information about the different ways it can occur and potential management strategies - examples include types of surveillance and information gathering through social media, cyber activity and relationship building.
- Internal guidance on the development of contracts, funding agreements, financial investments and partnerships involving international entities isdeveloped.
- Clear arrangements are in place for researchers to report concerns about foreign interference.
- Advice and support for researchers and HDR students is provided across a range of areas. This could include:
    - selective management of events such as academicforums;
    - safe travel arrangements (see Commonwealth Travel Guidelines); and
    - review human research ethics guidelines to manage high risk researchactivity.
- Maintain internal records of research funding arrangements with third party research partners.

3.2 Know your research staff and collaborators

Ideation and collaboration involve interactions between institutions, researchers and students. These activities offer opportunities for foreign interference because many collaborations begin with casual exchanges in organised and informal research environments such as conferences, symposia and workshops. Most researchers are very open to introductions and approaches from colleagues at such events. These interactions are often iteratively followed up with collaboration on informal, often undocumented research activities, which in turn may lead to the creation of intellectual property.

The nature of the research process – and its dependence on decentralised, personal interactions – means universities need to invest in developing the awareness among staff and HDR students about the need to assess risk.

I. The capacity of research staff and HDR students to assess risk in their research projects

While universities have processes in place to assess financial and other risks associated with international research collaborators or funders, researchers should also take reasonable steps to consider whether a potential contributor, employee or partner poses a risk, either reputational or security related, and to make decisions based on this assessment. This should take into account an awareness that foreign research collaborators may have undisclosed relationships or not be aware of the need to comply with jurisdictional requirements, such as trade controls.

DRAFT

Key considerations

- What training and awareness strategies are needed to ensure researchers understand the need to comply with the university's risk mitigation strategies?
- Are researchers, and their foreign partners, aware of their legal obligations in relation to some types of research, including conflicts of interests?

II. Contracts and donors

Foreign entities may seek to access or influence particular areas of research through various forms of funding arrangements and other inducements targeted at individual researchers. For further information, including key consideration and a checklist, refer to section 2.2 Good Governance.

Key considerations

- What processes exist in the university to identify research that may require additionaloversight?

Checklist

- Processes to identify research that may require additional oversight due to the nature of the research and/or the type of partnership.
- Consider the ways in which research integrity offices and security offices in universities could assist researchers in due diligence activities.
- Clear guidance on when researchers should seek further advice internally or external to the university.
- Clear requirements to undertake proportionate risk assessments at the startof international collaborative research projects.

3.3 Consider potential end-use possibilities

Universities and researchers need to be aware of the potential for down-stream impacts (not anticipated by the formal research project plan) of their research. Risk management strategies could include taking early steps to identify and protect certain technologies and research, and cultivating an open and transparent harm minimisation culture in the university. These systems draw a distinction between those technologies covered by the DTCA and those with the longer term potential to be used in ways that are not consistent with promoting economic, social and security benefits for Australians. These strategies should be targeted, appropriate and fit for purpose – where research has a low risk, the requirements on the researchers and governance systems should reflect this.

DRAFT

I. Dual–use technology and research

The DTCA provides the legislative basis for the control of supply, publication and brokering of defence and strategic goods and technology. Similarly, the *Customs Act 1901* and regulations regulate the transfer of tangible goods and technologies. These arrangements enable Australia to control the export of goods and technology to minimise the risk of them ending up in the wrong hands. Australia's legislative framework helps to ensure we are in line with international best practice.

Key considerations

- How do researchers reasonably consider the potential for their research to becomedual-use?
- What strategies are in place to ensure compliance with the defence trade controlsregime?

II. Potentially sensitive technology

Research can have many end-use applications that often cannot be identified in the early stages of development. Sometimes the difference between potential immediate uses for dual-use technology and determining the possible end-uses of some research can be a grey area for researchers and organisations.

Key considerations

- Do researchers consider the potential for their research to be used for purposes that are inconsistent with promoting economic, social and security benefits forAustralians?
- What strategies monitor the development of research in areas of potential high risk?

III. Active approach to IP partnerships

Research with potential commercial benefit can be of interest to foreign entities. Research theft and misappropriation can occur at any stage of the research process and intellectual property rights may be limited in protecting commercially valuable research. A risk management system will help to identify vulnerabilities to theft and misappropriation.

Key considerations

- What mechanisms does your university have to identify and protect commercially valuable research?
- What additional or targeted training is provided to researchers involved in commercially valuable research to minimise the risk of foreigninterference?

DRAFT

Checklist

- Processes to assess the risk of potential links between some areas of research andfuture dual-use technologies.
- Training for researchers to help them identify possible downstream applications of some research undertaken in collaboration with internationalentities.
- Assess whether particular areas of research might be a target for foreign interference or misappropriation.
- Regularly consult with the Department of Defence to seek advice regarding sensitiveand dual-use technologies and ensure compliance with exportcontrols.

DRAFT

Cyber Security

4.0 Objective

University digital ecosystems seek to thwart unauthorised access, manipulation, disruption or damage, and ensure the confidentiality, integrity and availability of information. These guidelines have been developed to assist universities to manage and protect their networks, as well as detect and respond to cyber security incidents should they occur.

4.1 Implementation of university cyber security strategies

Cyber security strategies can help universities to ensure they have the resources and capabilities to protect their information ecosystems. Tailored to the circumstances of individual universities, such strategies:

I. are based on an understanding of, and are proportionate to, the risks the university may face from cyber threats and potential vulnerabilities;

II. draw on existing frameworks such as the Information Security Manual (ISM), Essential 8 or National Institute of Standards and Technology to develop a coherent and complementary set of safeguards;

III. enhance sharing of strategies and expertise across thesector;

IV. assist to develop a core set of design and operational documents, policies and procedures (to guide risk identification and management);

V. inform how best to communicate their cyber security strategies to generate momentum and acceptance;

VI. encompass aspects of security culture, governance, supply chain, technical controls and data; and

VII. consider methods to track the progress and effectiveness of a university's cyber security strategy.

DRAFT

Checklist

- Each university has a cyber security strategy.
- Universities develop a set of foundational documents to support the implementation of individual cyber security strategies.
- Universities identify mechanisms to share insights, policies and expertise.
- Universities develop a set of common, core policies and procedures as partof their cyber security strategy, noting each university will have its owncustomisation.
- Universities consider ways to enhance talent development and retention of staffwith specialist expertise in government anduniversities.

4.2 Cyber-intelligence sharing across the sector and with Government

Sharing cyber intelligence between universities and with government helps to build a common picture of threats across the sector. This enables universities to respond to evolving risks from cyber-threats, share countermeasures and enable government to provide timely and tailored assistance. It will also help Australian government departments and agencies to gain a deeper understanding of the operational realities of the sector, and the practices that contribute to the success of our higher education and research system.

Universities are encouraged to:

I. share sensor data and other threat intelligence (however, the discretion to do so, and to what extent, always remains with each university);

II. participate in sector briefings and forums convened by the Australian Cyber Security Centre (ACSC) and other security agencies;

III. consider joint incident management arrangements with other universities, to help build surge capability;

IV. share insights on cyber security related technology choices;

V. consider secure methods of storing and transmitting shareablecyber-intelligence;

VI. ensure data sharing arrangements accord with the principles of privacy and any commercial considerations; and

VII. maintain a current list of government security agency contacts.

DRAFT

Checklist

- Government offers regular briefings on cyber security threats touniversities.
- Government establishes a contact register for universities to contact departmentsand agencies when needed.
- Universities share insights on cyber security related technology choices,including the potential formation of a sector cyber security panel for technologyacquisition.
- Universities have a point of coordination for cyber securitymatters.
- At the discretion of each university, share network sensor data and analytics across the sector and with government.
- Universities explore opportunities to develop a joint incident management protocolto provide surge capabilities between universities.

4.3 Cyber security as a whole-of-organisation “human” issue, with strong emphasis on a positive security culture

Nurturing a strong cyber security culture requires the willing support of students, staff, researchers and executives. This means embedding cyber-safe behaviours and decision making across the university and viewing cyber security as an essential enabler of academic freedom, student and staff safety and the university’s goals.

Universities will give care to:

I. calibrate cyber security messages and cultural change programs to the unique challenges and expectations of its different user groups i.e. researchers, staff, students andexecutives;

II. engage all levels of university structures, including councils, to help embed and drive a positive cyber security culture;

III. align cyber safe culture programs to the other elements of a university’s cyber security strategy;

IV. frame cyber security challenges and solutions through the lens of users notjusttechnology;

V. emphasise the overarching principle of collective and individual responsibility in a mature cyber safe culture;

VI. promote cyber security capabilities as an enabler and safeguard for academic freedom and free intellectual enquiry; and

VII. share approaches on creating and embedding cyber safety messages and practice mindful of the commonality of some cultural challenges, and the mobility of personnel between campuses.

DRAFT

Checklist

- Short courses for technical and cultural education for internal use across the sector.This includes potential gamification of aspects of cyber security.
- A collaborative cross-disciplinary user study to understand researcher and user behaviour characteristics to calibrate messaging and support cyber safe behaviour and decision making.
- Cyber safe pocket guides for different user cohorts could be a useful additionalresource.
- A physical and virtual cyber security simulation may assist to show how threat actors operate e.g. compromised USBs etc.
- Guest speakers from international universities share their experiences and approaches to cyber-safety.
- Involve council, executive and faculty/school decision makers in cybersecurity governance.

4.4 Cyber threat-models to understand and mitigate business risks

Threat-modelling is a proactive method to identify potential threats and the risks they pose to universities, so countermeasures can be developed and deployed. Well-developed threat-models allow the sector and individual universities to articulate business risks to feed into their strategy and to build a case for investment.

Elements of a strong model framework include:

I. regular guidance from ACSC and other security agencies to enhance understanding of the nature of the threats faced;

II. tie threat models to sources of threat intelligence; and regularly update to align to current and emergent threats;

III. encouragement for universities to share threat models with each other and government agencies to develop a common threat picture, and potential sector-widemitigations;

IV. threat models that help guide and refine university cyber security strategies as well as capability investment; and

V. threat models developed with input from a broad set of organisational ‘risk owners’. Training for risk owners and executives in threat modelling thinking may assist.

DRAFT

Checklist

- Threat models developed for the circumstances of individual universities, leveraging useful examples from other universities as well as guidance from ACSC.
- Drawing a common framework from individual university threat models to assist the sector in resources co-developed with government, and regularly updated.
- Trainer/practitioner workshops delivered to build threat-modelling capabilities.
- Threat-modelling guest speakers invited, to enhance threat model thinking andpractice.
- Individual and sector threat-models used to refine strategy, share intelligenceand build sector-wide capabilities.

DRAFT

Glossary

Academic solicitation	Academic solicitation is the improper attempt to obtain sensitive or classified information from students, professors, scientists or researchers.
Accountable authority	A senior representative responsible for particular areas of work, managingsensitivities.
Cyber security	Cyber security refers to the technical and people capabilities, leadership, culture, techniques and practices, which collectively protect an organisation's digital infrastructure; and to 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 the lack of investment in the hygiene of systems or infrastructure.
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, which are coercive, covert, deceptive or corrupting and are contrary to Australia's sovereignty, values and national interests.

DRAFT

Protective security	An organised system of measures to prevent risks from occurring.
Research	The concept of research is broad and includes the creation of new knowledge and/or the use of existing knowledge in a new and creative way so as to generate new concepts, methodologies, inventions and understandings. This could include synthesis and analysis of previous research to the extent that it is new and creative.
Risk	The possibility of a threat, danger, or the possibility of lost or compromised information, assets, or resources.
Safety	To be protected and free from a threat. To be used in reference to culture, physical protections, communication plans and public facing documentation.
Safety culture	Authentic consensus and understanding from an intended audience on why it is important to adhere to certain procedures and values regarding protection and freedom from a threat.
Security	To be protected and free from a threat. To be used in the context of government agencies, internal risk frameworks, protocols and procedures.
Sensitivity	Information that should be handled carefully by an organisation as it may cause unfavourable outcomes if not managed appropriately.
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 cyber security is a rapidly evolving discipline: you can create threat models for almost any scenario you canimagine. Successful threat modelling requires identifying potential threats, analysing the possible effects of those threats, and determining if the threat is significant and requires a neutralizationstrategy.

DRAFT

Acronyms

ABC	Anti-Bribery and Corruption
ACSC	Australian Cyber Security Centre
ANU	Australian National University
ASIO	Australian Security Intelligence Organisation
BGLU	Business and Government Liaison Unit
CoC	Conflict of Commitment
CoI	Conflict of Interest
CSSO	Chief Safety and Security Officer
DTCA	Defence Trade Controls Act 2012
HDR	Higher Degree Research
ISM	Information Security Manual
MoU	Memorandum of Understanding
NZ	New Zealand
Taskforce	University Foreign Interference Taskforce
UK	United Kingdom
US	United States
USB	Universal Serial Bus

DRAFT

Resources and guidance available

Including relevant legislation and frameworks. This section should be broken down into resources that cover all areas and resources that more specifically target one of the working groups.

Minister for Education press release - Establishment of a University Foreign Interference Taskforce

Australia's Counter Foreign Interference Strategy

Australian Government Information Security Manual

Essential Eight to ISM mapping

Travelling Overseas with Electronic Devices

Protect your organisation from phishing

Cloud Computing Security for Tenants

Defence Trade Controls Act 2012

Foreign Influence Transparency Scheme

Australian Code for the Responsible Conduct of Research (2018)

National Principles of Intellectual Property Management for Publicly Funded Research

Australian Research Council Intellectual Property Policy

ASIO Business and Government Liaison Unit

Australian Government Security Vetting Agency – Gold Standard Proof of Identity

Protective Security Policy Framework – fact sheets and publications

Medicines Australia – Code of Conduct

Security awareness campaigns – UK Centre for the Protection of National Infrastructure

Security Considerations Assessment - UK Centre for the Protection of National Infrastructure

Security planning – NZ Protective security requirements

DRAFT

Appendix 1 – Options for prioritisation guidance

DRAFT

Prioritisation guidance is intended to support decision makers balance priorities in building resilience to foreign interference.

The following matrix has been developed **outlining an example** of short term, medium term and long term desired outcomes and leads. It should be noted that no one size fits all approach to prioritisation is possible given the autonomous nature of universities, consideration of the proportionately of risk specifically relevant to a university and different circumstances.

Short term

Include foreign interference risks in existing policies, procedures and strategies, subject to an institutions circumstances.

Desired outcome	Lead	Reference (for further details)
University communication plans and education programs raise awareness of foreign interference risk.	Institutions	Culture and communications • Communication and education on foreign interference risks
Staff are supported by university processes that assist them to be mindful of foreign interference risks when collaborating with an international partner.	Institutions	Foreign collaboration • Know your partner
Before entering into a formal partnership agreement, due diligence is completed to establish who the partner is.	Institutions	Foreign collaboration • Know your partner
Universities have a Conflict of Interest policy which identifies foreign affiliations, relationships and financial commitments that may impact staff responsibilities to their Australian university.	Institutions	Foreign collaboration • Transparency and knowledge sharing
Researchers, professional staff and Higher Degree Research students' are aware of the ways in which foreign interference can occur.	Institutions Commonwealth	Research and IP • Proactive proportionate approach to risk
Regular guidance from ACSC and other security agencies to enhance understanding of the nature of the threats faced.	Australian Cyber Security Centre	Cyber security • Cyber threat models to understand and mitigate business risks

Share approaches on creating and embedding cyber safety messages and practices mindful of the commonality of some cultural challenges, and the mobility of personnel between campuses.	Sector	Cyber security • Cyber security as a whole-of-organisation 'human issue,' with strong emphasis on a positive safety and security culture
Participate in sector briefings and forums convened by the ACSC and other security agencies.	Institutions Australian Cyber Security Centre	Cyber security • Cyber-intelligence sharing across the sector and with government
Maintain a current list of government security agency contacts.	Institutions	Cyber security • Cyber-intelligence sharing across the sector and with government

DRAFT

Medium term

Implementing medium-term desired outcomes, planning, review, and subject to an institutions capability and maturity levels.

DRAFT

Desired outcome	Lead	Reference (further details)
Accountable authorities oversee security and safety risks and are responsible for risk mitigation strategies.	Institutions	Culture and communications • Accountable authorities
A Chief Safety and Security Officer (CSSO) or other senior executive as CSSO.	Institutions	Culture and communications • Accountable authorities
Universities incorporate into existing relevant frameworks foreign interference threats and vulnerabilities to the university's people, information and assets and outline mitigation measures.	Institutions Assistance can be provided by the Commonwealth	Culture and communications • Foreign interference risk planning
Universities regularly assess the comprehensiveness of their safety and security strategy, policies and procedures on foreign interference, and consider incorporating into risk reporting cycles.	Institutions	Culture and communications • Regular evaluation and review of foreign interference risk planning and mitigation for robust quality assurance
Before entering into a formal partnership agreement, due diligence is completed to establish who the partner is.	Institutions	Foreign collaboration • Know your partner
University policies and procedures that outline the requirements for staff, students, contractors and honorary staff engaging in international collaboration	Institutions	Foreign collaboration • Good governance
Universities build a repository of information on interference-associated foreign collaboration, which can be shared internally.	Institutions	Foreign collaboration • Transparency and knowledge-sharing
Interference-associated foreign collaboration risks that could have adverse impact broader than one university are shared across the higher education sector.	Sector	Foreign collaboration • Transparency and knowledge-sharing
Universities provide staff with access to channels, which reports threats of foreign interference to their university and the broader higher education sector.	Sector	Foreign collaboration • Transparency and knowledge-sharing

DRAFT

Transparent and robust reporting requirements further developed, documented and maintained.	Institutions	Research and IP • Proactive proportionate approach to risk
The capacity of research staff and HDR students to assess risk in their research projects.	Institutions	Research and IP • Know your research staff and collaborators
Dual–use technology and research.	Institutions	Research and IP • Know your research staff and collaborators
Potentially sensitive technology.	Institutions	Research and IP • Know your research staff and collaborators
Active approach to IP partnerships.	Institutions	Research and IP • Consider potential end-use possibilities
Cyber security strategies help universities to ensure they have the resources and capabilities to protect their information ecosystems.	Institutions	Cyber security • Implementation ofuniversity cyber security strategies
Data sharing arrangements accord with the principles of privacy and any commercial considerations.	Sector Australian Cyber Security Centre	Cyber security • Cyber-intelligence sharing across the sector with government
Consider joint incident management arrangements with other universities, to help build surge capability.	Sector Australian Cyber Security Centre	Cyber security • Cyber-intelligence sharing across the sector with government
Share insights on cyber security related technology choices.	Sector Australian Cyber Security Centre	Cyber security • Cyber-intelligence sharing across the sector with government
Calibrate cyber security messages and cultural change programs to the unique challenges and expectations of its different user groups i.e. researchers, staff, students and executives.	Institutions	Cyber security • Cyber security as a whole-of-organisation 'human issue,' with strong emphasis

		on a positive safety and security culture
Engage all levels of university structures, including councils, to help embed and drive a positive cyber security culture.	Sector	Cyber security • Cyber security as a whole-of-organisation 'human issue,' with strong emphasis on a positive safety and security culture
Frame cyber security challenges and solutions through the lens of users not just technology.	Sector	Cyber security • Cyber security as a whole-of-organisation 'human issue,' with strong emphasis on a positive safety and security culture
Emphasise the overarching principle of collective and individual responsibility in a mature cyber safe culture.	Sector	Cyber security • Cyber security as a whole-of-organisation 'human issue,' with strong emphasis on a positive safety and security culture
Promote cyber security capabilities as an enabler and safeguard for academic freedom and free intellectual enquiry.	Institutions	Cyber security • Cyber security as a whole-of-organisation 'human issue,' with strong emphasis on a positive safety and security culture
Encouragement for universities to share threat models with each other and government agencies to develop a common threat picture, and potential sector-wide mitigations.	Sector Commonwealth	Cyber security • Cyber threat models to understand and mitigate business risks

DRAFT

Long term

Cultural awareness, evaluation and review, subject to a university’s capability.

Desired outcome	Lead	Reference (further details)
For collaborations that continue over an extended period, due diligence assessments of partners are revisited and formal agreements subject to regular review.	Institutions	Foreign Collaboration • Know your partner
Contracts and donors.	Institutions	Research and IP • Know your research staff and collaborators
Consider methods to track the progress and effectiveness of a university’s cyber security strategy.	Institutions	Cyber security • Implementation ofuniversity cyber security strategies
Share sensor data and other threat intelligence (however, the discretion to do so, and to what extent, always remains with each university.	Institutions Commonwealth	Cyber security • Cyber-intelligence sharing across the sector and with government
Tie threat models to sources of threat intelligence; and regularly updated to align to current and emergent threats.	Institutions Commonwealth	Cyber security • Cyber threat models to understand and mitigate business risks
Threat models that help guide and refine university cyber security strategies as well as capability investment.	Institutions	Cyber security • Cyber threat models to understand and mitigate business risks
Threat models developed with input from a broad set of organisational ‘risk owners.’ Training for risk owners and executives in threat modelling thinking may assist.	Institutions	Cyber security • Cyber threat models to understand and mitigate business risks

DRAFT

Appendix 2 – Scenarios

The following scenarios have been developed to guide staff, researchers and decision makers in the identification of foreign interference activities.

Research and IP

What training assists researchers to identify trigger-points in the research process where foreign interference may occur?

Informal (and sometimes formal) research activities often commence with a discussion or conversation and progress at variable rates to different levels of engagement and involvement.

A researcher may find themselves involved in collaboration in a step-by-step fashion rather than as a single point-in-time decision.

Researchers may also have strong collaborations with individuals and groups that consist as a range of formal and informal activities, which further complicates the governance of any particular activity at a particular time. This gradual sequencing of activities provides a context conducive for foreign interference actors to operate in.

A typical sequence might be that a researcher, having read papers by a colleague, meets them at a conference where the other researcher lives and agrees to visit their lab/research group. The visitor gives an impromptu seminar and spends time with graduate students. As a result, a student receives helpful advice and the researchers agree the student will travel to the other location to future develop the ideas/assistance. This eventually results in co-authorship of one or more papers and acknowledgment on the student’s thesis.

It is subsequently discovered that the project was funded by the military of the foreign government and that the research project outcomes were used to assist that government in its own national interests and against those of Australia.

DRAFT

Research and IP

How do researchers assess and reassess their involvement in activities along the research pathway?

Informal research activities result in outputs (such as papers or other tangible products) and/or outcomes (effects). Researchers are asked to think through the impacts that could follow from both outputs and outcomes.

For example, an *output* from discussions with a PhD student in a lab at University X a researcher is proposing to visit may be the design and description of an algorithm; a follow-on *outcome* might be that the student is able to implement the algorithm and overcome a hitherto unpassable obstacle. This has the *impact* of advancing the student's candidature and is of sufficient significance that the researcher is invited to participate as a co-author on a joint paper with the student and their advisor. At this point an assessment should be made of the potential uses of the research and whether it may be put to uses contrary to institutional principles or our national interest. In cases such as this, it is clearly challenging to predict in advance whether a visit will be meaningful in the way the example describes. This is why researchers constantly gauge whether their involvement in activities should be reassessed for whether they should proceed at all or whether they should formalise the activity.

Research and IP

How do researchers take a risk management approach from the beginning of their research projects, particularly if the research involves potential high-value applications or technology?

Researcher X has been working for a number of years on an application that will enable the smarter use of new energy technology, with the potential for commercial application across Europe where there are many countries with well-developed renewable energy systems. One day the researcher is alerted to a media article about a start-up in country X that plans to revolutionise the renewable energy sector with the launch of a new application. Researcher X discovers that two of the company directors are known to him – one was a post-graduate student who spent a short period of time under his supervision, and the other an academic he met at a conference and went on to regularly exchange papers and ideas with.

DRAFT

Foreign collaboration

A foreign company (the company) approaches a university with a proposal to fund a research centre, building on research already underway in the university. The research is into an emerging technology with dual-use application – useful in both military and civilian domains. The proposal includes lease of a building, provision of research, technical and administrative staff, supply of equipment and additional funds for academic staff at the university to further their research in the area.

The proposal includes agreement that unused space in the leased building may be released at the sole discretion of the company, that the company's research, technical and administrative staff will be granted "typical" university access to places and systems (e.g. afterhours access to buildings, university staff network accounts), and that the centre will be "co-directed" by an academic leader and a company representative. The proposal also specifies that in the event of a dispute, resolution will take place in the jurisdiction where the company resides.

How might a university navigate such circumstances? Areas where risk would arise in the above example would include:

- The university's loss of control over tenants in a building housing dual use application technology.
- The granting of "typical" access to places and systems makes other research at the university vulnerable and places a university's employees and student information atrisk.
- Will company staff have access to the internal telephone and email directory for the university?
- The presence of leadership, research, technical and administrative staff not bound by the university's employment agreement, codes of conduct or values of academicfreedom.
- Dispute resolution in a foreign jurisdiction may severely limit the capacity of the university to receive a fair hearing on the matter.

To undertake due diligence, the university needs information about the company. This would include details of ownership and management, business registration information and company background, as well as the background and identifying details of the company's board members and directors. The company should disclose any history of legal issues in respect of regulatory, criminal or civil matters in order for the university to assess the risk. References from other business partners can provide useful verification of how the company approaches relationships.

In this scenario, on gaining the requested information, the university retains the services of a professional risk advisor to examine and analyse the information supplied and provide additional assurance. The professional risk advisor seeks to answer, for example, questions like:

- How "real" is the company and what is its businesshistory?
- Does it, or its board members and directors, have a history of insolvency or bankruptcy; litigation; involvement in corruption, bribery or graft; or intellectual property infringement and theft?
- What is the company structure and do any potential conflicts of interestexist?
- Is there any indication that a foreign State could exert control over thecompany?
- Does it, or its board members and directors, have any known or suspected association with serious or organised crime groups, money laundering groups, terrorist groups or foreign intelligence services?

DRAFT

In seeking further information on the company, the professional risk advisor identified that the beneficial ownership of the company effectively made it a wholly owned subsidiary of a State Owned Enterprise residing in a different country altogether. This country's government was guided by principles that could not be described as free, open or democratic.

The subsidiary – the company – seeking to engage with the university, however, was based in a country with strong traditions of democracy and rule-of-law. In addition, referee reports from others who have collaborated with the company attest that it is has been scrupulous in meeting its agreements.

On the basis of this due diligence – and cognisant of the higher background risk – the university decides to proceed to negotiate with the company. Priority elements of the proposal that need changing in order to mitigate the most severe of the identified risks include:

Defining the jurisdiction where dispute resolution will occur to be the one the university operates in;

- Introducing the university's policies, standards, regulations and codes of conduct into the contract in a way that is legally binding.
- Reserving the right to veto a proposed tenant in the leasedbuilding.
- Restricting company staff to a dedicated network hosted within the collaborationarea.

Additionally, the university adopts an approach of continuous risk assessment for the collaboration with the company to ensure it makes itself aware of any changes to the risk profile. It also devises an exit strategy from the collaboration and builds this into the contract.

DRAFT