GUIDELINES TO COUNTER FOREIGN INTERFERENCE IN THE AUSTRALIAN UNIVERSITY SECTOR

University Foreign Interference Taskforce
November 2019

ACKNOWLEDGEMENTS

The following individuals and organisations are acknowledged for their contributions to the development of the guidelines.

- The Steering Group made up of:
  - Chris Teal, National Counter Foreign Interference Coordinator, Department of Home Affairs – Chair
  - Cameron Ashe, Acting National Counter Foreign Interference Coordinator, Department of Home Affairs – Acting Chair
  - Martin Bean CBE, Vice-Chancellor, RMIT University – Deputy Chair
  - David Learmonth, Deputy Secretary Higher Education, Research and International, Department of Education
  - Catriona Jackson, CEO, Universities Australia
  - Vicki Thomson, Chief Executive, The Group of Eight
  - Professor Alex Zelinsky AO, Vice-Chancellor, University of Newcastle
  - Professor Peter Høj AC, Vice-Chancellor, University of Queensland
  - Professor John Dewar, Vice-Chancellor, La Trobe University
  - Rachel Noble PSM, Head of the Australian Cyber Security Centre
  - Sarah Chidgey, Deputy Secretary Integrity and International Group, Attorney-General's Department
  - Heather Cook, Australian Security Intelligence Organisation
  - Professor Tanya Monro, Chief Defence Scientist, Department of Defence.
- Four working groups, established under the Steering Group, co-chaired by a government and a sector representative, expertly drafted content on key strategic areas.
- The university sector for their participation and extensive collaboration throughout the process.

Australian Government

UNIVERSITIES AUSTRALIA

GROUP OF EIGHT AUSTRALIA

CONTENTS

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. A cyberattack on the Australian National University in 2018 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.

Following a meeting in Wollongong convened by the Australian Minister for Education, the Hon Dan Tehan MP, 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 on emerging threats.

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.

The overarching principles guiding the taskforce were:

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

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, noting universities will always endeavour to achieve the best possible outcomes.

The threat environment

In October 2019, Australia's Director-General of Security, Mr Mike Burgess, noted the unprecedented scale of foreign interference activity against Australia's interests.[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.

'Foreign interference' versus 'foreign influence'

Foreign interference

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

Foreign influence

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

A proactive approach by the university sector to the threat of foreign interference helps to safeguard the reputation of Australian universities, protect academic freedom, and ensure our academic institutions and the Australian economy can maximise the benefits of research endeavours. Such a response is consistent with Australia's Counter Foreign Interference (CFI) Strategy, which aims to increase the cost and reduce the benefit to foreign governments of conducting foreign interference in Australia.

The majority of international interactions are welcome and to Australia's benefit. However, there may be foreign actors who seek to engage in foreign interference in the university sector, through:

- efforts to alter or direct the research agenda;
- economic pressure;
- solicitation and recruitment of post-doctoral researchers and academic staff; and
- cyber intrusions.

Due to the unprecedented risks of foreign interference, in mid-2019, universities and Government agencies had discussed further collaboration. In August 2019, the Hon Dan Tehan MP, Minister for Education, announced the establishment of the University Foreign Interference Taskforce to develop guidelines to counter foreign interference in the university sector. Further details are provided in Appendix 1.

These guidelines contribute to the building of greater resilience to these threats in the Australian university sector, without compromising global collaboration.

[1] ASIO, Director General's Senate Estimates, https://parlinfo.aph.gov.au/parlInfo/download/committees/estimate/48ea734a-e5f8-4bc6-813e-1f22b32a238a/toc_pdf/Legal%20and%20Constitutional%20Affairs%20Legislation%20Committee_2019_10_21_7290.pdf;fileType=application%2Fpdf#search=%22committees/estimate/48ea734a-e5f8-4bc6-813e-1f22b32a238a/0000%22

INTRODUCTION

Universities play a key role in the development of new knowledge and technological innovation. This is vital to continued productivity and economic growth. University autonomy includes a proactive approach to manage and engage with risk, supported by the Government and security agencies, mindful of the national interest. The guidelines are intended to further empower institutions in a way that is both durable and responsive to emerging threats and pressures as these develop and change over time.

Australian universities are deeply engaged internationally, sharing and developing knowledge with the best and brightest minds around the world. Australians benefit significantly from the flow of information and intellectual property. The international nature of collaboration is vital to research and the generation of world leading research. Careful consideration is given to the potential tensions between developing institutional policies to protect against the risk of foreign interference, while also promoting the free exchange of ideas, an open research culture and academic freedom.

The Australian higher education sector is taking a leadership role, in partnership with the Australian Government, to ensure the sector continues to be an attractive research and education partner while mitigating unintended risks.

Universities conduct research into a wide array of fields, from the arts to social sciences, medical breakthroughs to engineering and information technology. It is important to consider the proportionality of the risk and the scale of the response in diverse fields of research.

Proportionality of risk underlines the guidelines. The majority of international interactions are to Australia's benefit, and the guidelines are not intended to inhibit the majority of academic activities, which are low risk.

Upholding the foundational principle of university autonomy, a number of key themes guide this work to deepen resilience against foreign interference. Universities have already made significant investment in the development of sophisticated risk management frameworks and associated policies and practices, including the management of risk associated with international collaboration and engagement. The key themes and objectives to manage and engage with risk and best practice considerations provided in these guidelines are intended to build upon this base.

Key themes include:

Governance and risk frameworks

- Ensuring structures promote and strengthen a positive safety and security culture, which builds resilience to foreign interference.
- Including foreign interference risks in existing risk frameworks, policies and procedures and identifying capabilities in the university that contribute to the security of people, information and assets.

Due diligence

- Applying due diligence proportionate to the risk.
- Making considered risk assessments based on the combined sensitivity of the research topic and potential research partner.
- In addition to internal governance requirements, university policies and procedures also ensure consideration is given to whether legislative frameworks like the *Defence Trade Controls Act 2012 (DTCA)* and the *Foreign Influence Transparency Scheme Act 2018* apply.
- Knowing your partner, research collaborators and staff by undertaking appropriate due diligence, supported by university processes, taking account of the potential foreign interference and reputational risks.

Communication and education

- Communicating the risk of foreign interference, acknowledging that often the risk is low.
- Communication strategies and education programs raise awareness of foreign interference risks, and arm decision makers with knowledge to enable levels of vigilance proportionate to the risk.
- Communication strategies, education and professional development programs promote the university's commitment to security culture, and raise awareness of risks and their implications.

Knowledge sharing

- Strengthening knowledge sharing mechanisms across the sector and between the sector and the Commonwealth, about emerging risks and experiences of foreign interference.
- The need for security agencies to provide greater assistance to universities to identify risks and proportionate responses is acknowledged, noting significant information is already available to universities.

Cyber security

- Protecting information held on ICT systems through the development and implementation of robust cyber security strategies, engaging with Commonwealth agencies, sharing best practice and cyber threat modelling.

HOW TO USE THESE GUIDELINES

These guidelines recognise university autonomy. They are not intended to be prescriptive. Key themes and objectives have been identified to help manage and engage with risk to deepen resilience against foreign interference. Best practice considerations supplement the key themes and objectives to further assist decision-makers in their risk management.

Universities already have policies, frameworks, systems and processes to ensure a positive 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 risk mitigation strategies.

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

The document has two sections.

- key themes and objectives to assist universities manage and engage with foreign interference risk; and
- best practice considerations to assist decision-makers, which will evolve over time.

Key themes and objectives are:

- underpinned by an **objective statement** to manage and engage risk to deepen resilience against foreign interference;
- **supported by questions, which are not intended to be prescriptive,** but designed to guide universities in addressing the range of emerging risks in global higher education arising from foreign interference appropriate to their own context; and
- intended to **support an environment of trust and confidence** across the university sector to guide decision-making based on proportionality of risks and an environment of continuous improvement.

Best practice considerations:

- provide more specific guidance to **assist decision-makers** address key themes and objectives;
- are **evolving and subject to continuous improvement**, including further supplementation of university sector best practice considerations;
- aimed to **assist decision-makers to enhance a positive security culture** to help safeguard against foreign interference;
- intended to support decision-makers **balance priorities proportionate to the risk** and acknowledge the different capability and maturity levels across the sector; and
- **not intended to impose additional compliance or regulatory burden**. Universities may determine how best practice considerations may be applied and incorporated given their operations and proportionality of risk.

GOVERNANCE AND RISK FRAMEWORKS

Objective

Universities have policies, structures, and frameworks in place to promote and strengthen a culture of security, and resilience to foreign interference.

Accountable authorities

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

A strong security culture depends on active leadership, communication and authentic determination from the right people – it is not a short-term project. An accountable authority is a senior executive or executive body, responsible and accountable for the security of people, information and assets to counter foreign interference.

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 security culture to foster individual responsibility to manage such risks.

Questions to guide decision-making

- Who in your university has operational responsibility for foreign interference and safeguards?
- What university policies and 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 policies does your university have that trigger engagement with relevant Commonwealth agencies on legislative compliance and foreign interference?

Foreign interference risk planning

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

Universities already have policies, frameworks, systems and processes to ensure a positive security 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. Integrating foreign interference risks in existing risk frameworks, policies and procedures promotes a strong security culture and avoids unnecessary duplication.

Consistent internal reporting mechanisms enables the sharing of security reporting, as appropriate, with Government agencies to enhance understanding of the security environment in universities.

Questions to guide decision-making

- 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 security policies and procedures?
- What policies 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 in a particular research project, and the nature of the governance and oversight that could be applied to mitigate this risk considered?
- What documentation and templates capture these considerations, and can be referred to, should a retrospective assessment of the research activity be undertaken?

University policies and procedures outline the requirements for staff, students, contractors and honorary staff engaging in international collaboration, proportionate to the risk

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, where required, with the DTCA and other regulations.

Questions to guide decision-making

- What mechanisms assist staff to identify and mitigate possible risks?
- 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 training is offered for researchers and Higher Degree Research (HDR) students to understand the need to comply with the university's risk mitigation strategies?
- What training and awareness strategies are needed to ensure researchers understand the need to comply with the university's risk mitigation strategies?
- To what degree are researchers, and their international partners, aware of their legal obligations, in some types of research, including conflicts of interests and complying with legislative requirements.
- What processes ensure staff are aware of their rights and obligations at the university and under Australian law?

Clear university risk assessment and reporting frameworks

Core to the management of foreign interference is the identification and management of risk. Universities 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:

- 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 be undertaken.

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

Questions to guide decision-making

- How robust are your risk framework mitigation strategies that deal with foreign interference in research?
- Who is responsible for maintaining, promoting and applying these arrangements?
- How are these arrangements informed by the range of research undertaken in the university and the associated level of risks?
- What ability and capacity does the university have to analyse and respond to the information gathered from internal reporting arrangements?
- What minimum level of due diligence is applied to foreign investments and partnerships at all levels?
- What level of internal reporting is in place for foreign investments and partnerships and does this aid accountability and risk management?

Transparent and robust reporting requirements are developed, documented and maintained

Those seeking to interfere with, or exert undue influence on, Australia's research effort may attempt inappropriately to alter or direct the research agenda into particular areas of research. This can occur through subtle forms of undue 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 build the capacity for early awareness and transparency among the university's stakeholders.

Questions to guide decision-making

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

Universities have a Conflict of Interest (CoI) policy/disclosure of interests policies, which identifies foreign affiliations, relationships and financial commitments and sets 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.

Questions to guide decision-making

- How do the university's CoI policies include international financial and other interests?
- How do the university's CoI policies 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.

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

University risk management strategies and tools improve with regular revision of lessons learnt, as well as through understanding and adapting to the security environment. Without review, education and communications cannot be targeted or relatable to a particular audience.

Questions to guide decision-making

- How consistent are internal reporting mechanisms to support internal evaluation and communication with external stakeholders?

DUE DILIGENCE

Objective

Universities need to know their partners through appropriate due diligence informed by knowledge of foreign interference risks. It is recognised that universities and government work in partnership on due diligence activities that consider proportionality of risk and availability of information sources.

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. 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.

Know your partner

Staff are supported by university policies that assist them to be mindful of foreign interference risks when collaborating with an international partner

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. University processes that inform staff about foreign interference risks can help them to do so.

Questions to guide decision-making

- 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 policies where appropriate?
- How are academic staff, professional staff and research students required to undertake training to recognise foreign interference risks in everyday work, communications and international travel?

Due diligence, proportionate to the risk and subject to information sources, is completed to establish who the partner is before entering into a formal partnership agreement

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.

Questions to guide decision-making

- 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 a project?
- What information or advice is available from government to assist?
- 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?
- What are the partner entity's relationships with foreign governments, political parties and related entities and individuals? Are these appropriately disclosed, for example is the information available to the public through a website or register such as the Foreign Influence Transparency Scheme register?

Institutional risk management frameworks are cognisant and responsive to activities covered by federal and state legislation, regulations and codes of conduct

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 DTCA and Autonomous Sanctions legislation and the *Foreign Influence Transparency Scheme Act 2018*.

Questions to guide decision-making

- How does the partnership consider potential internal and external risks to the university where it may be appropriate to obtain executive advice and approval?
- 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 DTCA?
- Does the activity or partnership proposed need to be registered under the Foreign Influence Transparency Scheme?

For collaborations that continue over an extended period, due diligence assessments of partners, proportionate to the risk and subject to information sources, are revisited and formal agreements are subject to regular review

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

Questions to guide decision-making

- Have collaborators' behaviours, interests and external relationships changed over time into something with which the university or individual is not comfortable?
- Has the government's advice or assessments changed over time?
- 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?

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

While universities have policies and processes 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.

Questions to guide decision-making

- What training and awareness strategies are there 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 some types of research, including conflicts of interests?

Robust agreements

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 collaboration are explicitly articulated

For all formal interactions with foreign institutions or individuals, best practice contracting mechanisms and policies reduce the risk of foreign interference. Terms and conditions of agreements or Memoranda of Understanding (MoUs) 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.

Questions to guide decision-making

- 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 primary partner.
- 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?
- Do contracts provide for the primacy of Australian laws?

Philanthropy and donations

Foreign entities may seek to access or influence particular areas of activity through various forms of funding arrangements and other inducements targeted at individuals.

Questions to guide decision-making

- What processes exist to manage risk when considering the acceptance of donations and gifts?

Research and intellectual property

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.

Universities already have robust research offices to help identify, develop and manage their intellectual property. An educative and policy response for Australian researchers that participate in the international research system is important to research training. Enabling the research community to recognise and respond to these growing trends while maintaining the openness that underlies the success of the Australian research sector is vital to guard against foreign interference while protecting the intentional reputation of Australia's universities.

Core to the management of foreign interference is the identification and management of risk. Universities 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.

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

Questions to guide decision-making

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

Research contracts

Foreign entities may seek to access or influence particular areas of research contracts through various forms of funding arrangements and other inducements targeted at individuals.

Questions to guide decision-making

- What policies exist in the university to identify research contracts that may require additional oversight due to the nature of the research and/or the type of partnership?
- How clear are requirements to undertake proportionate risk assessments at the start of international collaborative research projects?
- How could research integrity offices and security offices in universities assist researchers in due diligence activities?
- What guidance exists on when researchers should seek further advice internally or external to the university?

Consider potential end-use possibilities

It is not possible to predict all potential end use applications of research. However, risk management strategies can include taking early steps to identify and protect potentially sensitive technologies and research, and cultivate 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.

Dual–use technology and research

The DTCA provides the legislative framework 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.

Questions to guide decision-making

- How do researchers reasonably consider the potential for their research to become dual-use?
- What strategies are in place to ensure compliance with the defence trade controls regime and other relevant legislative frameworks?

Potentially sensitive technology and research outcomes

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.

Questions to guide decision-making

- Do researchers consider the potential for their research to be used for purposes that are inconsistent with promoting economic, social and security benefits for Australians?
- What strategies monitor the development of research in areas of potential high risk?
- What information or advice is available from Government?

Active approach to IP partnerships

Research with potential commercial benefit can be of interest to foreign entities, noting much research does not need to be protected and is openly shared. However, 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.

Questions to guide decision-making

- 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 foreign interference?

COMMUNICATION AND EDUCATION

Objective

The nature of research and academia can offer multiple entry points for potential foreign interference. Universities with assistance from Government agencies, provide training to staff and Higher Degree Research (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.

Promote communication and educative programs

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

Authenticity of security culture stems from embedded responsibilities and shared knowledge of university staff and students. Communication plans and education programs enhance a robust security culture and awareness of foreign interference risks.

Questions to guide decision-making

- 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?
- How can current university policies, for example pertaining to 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 manage their risks?

Researchers, professional staff and HDR students are aware of the ways in which foreign interference can occur

The nature of research can offer 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 negative consequences?
- How might they be affected?
- What might be affected by this research – positive and negative consequences?
- University guidelines and advice could adapt existing security and personal safety protections as required.

Questions to guide decision-making

- What training currently exists?
- How is training appropriately targeted to provide information about the more subtle forms of foreign interference?

KNOWLEDGE SHARING

Objective

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

The university sector already shares information amongst the sector as well as with the Government. Additional knowledge sharing mechanisms could be developed to address emerging risks and experiences of foreign interference. This includes sharing examples of foreign interference, attempts to exert undue influence, or otherwise undermine academic freedoms and values. The need for security agencies to better provide assistance to universities to identify risks and proportionate responses is acknowledged, noting information is already available to universities. A list of Government agency contacts is located at Appendix 2.

Sharing information between universities and with the Commonwealth

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

It is acknowledged that the university sector already shares information amongst the sector as well as with the Australian Government.

Where there is a risk that could affect the broader sector, institutions 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.

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. A reporting mechanism, or designated officer, to liaise with government enables a two-way avenue of communication about risks.

Questions to guide decision-making

- How does your university collaborate and share information across the sector?
- Do staff have ready access to information on potential partners that have engaged with the university in the past?
- Do staff know when and where to seek advice when they have concerns?
- How are experiences shared to help others and what opportunities are there to provide feedback and share lessons learned?

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. Liaison between universities and government agencies on security is typically done by an existing designated member of the executive team.

Questions to guide decision-making

- How do staff understand what risks should be shared with government agencies?
- How do staff know who their university contact is for liaison with government agencies?
- How does your university collaborate and share information with government?

CYBER SECURITY

Objective

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

Implementation of university cyber security strategies

Cyber security strategies can help universities to ensure they have the resources and capabilities to protect their information systems.

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.

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 security and the university's goals.

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.

BEST PRACTICE CONSIDERATIONS

This section is not intended to be prescriptive; it is intended to provide specific considerations to which decision-makers can refer, appropriate to their circumstance, to address key themes and objectives.

Best practice considerations are to be subject to continuous improvement. Over time, it is anticipated this will evolve with further examples of best practice from across the sector.

This section is not intended to impose additional compliance or regulatory burden. Universities may determine how best practice considerations may be applied and incorporated given their operations and proportionality of risk.

Governance and risk frameworks

The two key areas for governance and risk frameworks are:

- accountable authorities; and
- foreign interference risk planning.

This section provides examples of how a university may choose to manage these areas.

Accountable authorities

An accountable authority has responsibility and accountability for:

- the security of people, information and assets to counter foreign interference;
- overseeing the university's risk reporting framework to reflect its 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.

Some universities may embody these responsibilities in a Chief Safety and Security Officer. Other institutions may task an executive or other senior staff across different portfolios.

This role may include the following responsibilities:

- liaising between the university and Government agencies on security;
- supporting the accountable authority in the university to ensure the safety and security of people (including staff, students, contractors, visitors and clients), information and assets;
- 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 government agencies.

Foreign interference risk planning

The following are examples of ways in which foreign interference risk planning and mitigation measures could be incorporated into existing relevant frameworks:

- Clear mechanisms for staff and students to report foreign interference with oversight by the accountable authority/ies.
- Regular review of processes, guidance and communications for the security of people, information and assets for overseas travel with the risk of foreign interference in mind.
- Fully integrated protective security in planning, selecting, designing and modifying facilities for the protection of people, information and physical assets.
- Robust processes to remove systems access for university staff and students after they leave the university with the risk of foreign interference in mind.
- Physical security measures that minimise or remove the risk of:
  - harm to people, and
  - information and physical assets being rendered inoperable or inaccessible, or being accessed, used or removed without authorisation.

The following are examples of how universities policies and procedures can outline how staff, students, contractors and honorary staff can engage in international collaboration, proportionate to the risk:

- Staff follow university processes for 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 Australian legislation like the DTCA and the *Foreign Influence Transparency Scheme Act 2018*.
- Policies and processes for staff to report issues or to discuss concerns.
- 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 social agenda.
  - Demands – or inducements – to grant unnecessarily broad access to the university's information systems.
  - Use of acquired access to provide access to unapproved third parties.
  - 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 or dissent.
  - 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 are reported to the accountable authority/ies or relevant senior line manager. These matters may then be raised with Government agencies.

The following are considerations for a robust risk assessment and reporting framework:

- Training in foreign interference. 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.
- Clear arrangements for researchers to report concerns about foreign interference.
- Advice and support for staff and students is provided across a range of areas. This could include:
  - selective management of events such as academic forums;
  - safe travel arrangements (see Commonwealth Travel Guidelines); and
  - human research ethics guidelines to manage high risk research activity.
- Internal records of research funding arrangements with third party research partners.

The following are examples of ways in which universities manage conflicts of interests and disclosures of interest that identify international affiliations, relationships and financial arrangements:

- Provide appropriate, internal reporting of funding sources to help avoid reputational damage and better manage perception of undue influence or interference.
- Procedures ensure donations from international companies or Australian-based companies with strong foreign links are consistent with the university's policies, place no undue influence on the academic program, and are appropriately disclosed including through the Foreign Influence Transparency Scheme if required.
- The university's policies include advice on international travel, staffing appointments and engagements, and bribery, corruption, foreign donations and gifts.
- The Australian government Department of Foreign Affairs and Trade provides regularly updated travel advice for individual countries. www.smartraveller.gov.au
  - Anti-Bribery & Corruption 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 and forums.
  - The BGLU website operates on a free subscription basis.It has intelligence-backed reporting and resources. To subscribe: https://www.bglu.asio.gov.au/

The following are ways in which universities can regularly assess the maturity of their security strategy, policies and procedures as they relate to foreign interference:

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

Due diligence

The three key areas for due diligence are:

- know your partner;
- robust agreements; and
- research and intellectual property.

This section provides examples of how a university may choose to manage these areas.

Know your partner

The following are examples of how a university manages collaborations that continue over an extended period of time:

- Due diligence activities to help check that the proposed activities comply with the university's policies on academic freedom; audit and risk; research ethics and integrity, as well as relevant legislation.
- 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.
- Processes to guide the university to review the ethical, security, legal and reputational risks involved.
- Visibility of sensitive international travel, to assist in due diligence of risk while staff are overseas.
- A clear point of contact to seek advice or support for engagement activities.

Robust agreements

The following are examples of due diligence in international collaborations, contracts, partnerships or alliances:

- Foreign collaboration and ethical, security and reputational risks as an important, regular agenda item for meetings of senior staff.
- Senior executives have visibility of collaboration agreements, which streamlines governance, oversight, due diligence and risk assessment.
- Senior university executives have visibility of all formal collaboration agreements. A central registry (or similar) of international collaboration agreements could bring consistency and oversight to such engagements, and streamlines governance, due diligence and risk assessment.
- Consideration should be given to whether or not an arrangement is to be legally binding or non-binding such as an MoU, International Cooperation Agreement or other form of contract.
- Agreements with foreign partners 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.
- Universities review agreements regularly including to assess new risks and potential vulnerabilities that may have emerged during an international collaboration.
- Internal training and awareness sessions help manage international engagement including visits and foreign delegations.

The following are examples of ways in which universities can manage risks associated with philanthropy and donations:

- 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.

Research and intellectual property

The following are examples of due diligence in relation to research and intellectual property:

- Policies and processes to assess the risk of potential links between some areas of research and future dual-use technologies.
- Training for researchers to help them identify possible downstream applications of some research undertaken in collaboration with international entities.
- Assessment of particular areas of research which might be a target for foreign interference or misappropriation.
- Regular consultation with the Department of Defence to seek advice regarding sensitive and dual-use technologies and ensure compliance with export controls.

Communication and education

This section provides examples of how a university may choose to manage communication and education.

Promote communication and education programs

The following are examples of how university communication plans and education programs can raise awareness of foreign interference risks:

- A communication strategy which promotes the university's commitment to security culture, and raises awareness of the risk and its implications.
- Education and professional development programs which integrate awareness on foreign interference risk and mitigation.
- Targeted training for key personnel who contribute to the security of people, information, and assets to safeguard against foreign interference.
- Regularly reviewed communication plans and education programs on foreign interference.

Cyber security

The key areas for cyber security are:

- implementation of university cyber security strategies;
- cyber-intelligence sharing across the sector and with government;
- cyber security as a whole-of-organisation "human" issue, with strong emphasis on a positive security culture; and
- cyber threat-models to understand and mitigate business risks.

This section provides examples of how a university may choose to manage these areas.

Implementation of university cyber security strategies

University digital systems provide a platform to enable and support teaching, research, administration and engagement. They are designed and operated to thwart unauthorised access.

Cyber security strategies can help universities to ensure they have the resources and capabilities to protect their information systems. 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 the sector;
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.

The following are examples of ways in which universities implement cyber security strategies:

- Each university has a cyber security strategy.
- Universities maintain 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 policies and procedures as a component part of their cyber security strategy, noting each university will have its own customisation.
- Universities consider ways to enhance talent development and retention of staff with specialist expertise in government and universities.

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 shareable cyber-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.

The following are examples of ways in which universities can share cyber-intelligence across the sector and with Government:

- Regular briefings on cyber security threats to universities by Government.
- A contact register for universities to contact departments and agencies when needed.
- Insights on cyber security related technology choices shared, including the potential formation of a sector cyber security panel for technology acquisition.
- Point of coordination for cyber security matters.
- Share network sensor data and analytics across the sector and with government, at the discretion of each university.
- Explore opportunities to develop a joint incident management protocol to provide surge capabilities between universities.

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.

Consideration 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 and executives;
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 not just technology;
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.

The following are examples of ways in which universities can encourage cyber security as a whole of organisation issue:

- 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.
- A physical and virtual cyber security simulation to show how threat actors operate e.g. compromised USBs etc.
- Guest speakers from international universities share their experiences and approaches to cyber security.
- Council, executive and faculty/school decision makers are involved in cyber security governance.

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-wide mitigations;

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.

The following are examples of ways in which universities use cyber threat models to understand and mitigate business risk:

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

APPENDIX 1: UNIVERSITY FOREIGN INTERFERENCE TASKFORCE

In mid-2019, universities and Government agencies began consideration of further collaboration. On 28 August 2019, the Hon Dan Tehan MP, Minister for Education, announced the establishment of the University Foreign Interference Taskforce (the taskforce).

The taskforce brought together the university sector and Australian Government agencies to develop guidelines to counter foreign interference in the university sector.

A steering group was established to lead the taskforce. It involved equal representation from senior government officials and senior university representatives with relevant expertise.

Four working groups were established. Each focussed on a key strategic area. The working groups were co-chaired by the sector and the Government and contained further relevant experts from both the government and university sector.

The key strategic areas of focus included:

- culture and communication;
- foreign collaboration;
- research and intellectual property; and
- cyber security.

Australian universities engage broadly in international engagement, including research collaborations and education communities. The results of these engagements bring considerable benefit to Australia and Australian society. Universities take their position and responsibilities as a national asset very seriously, and reflect the academic freedom essential to universities.

The overarching principles guiding the taskforce were:

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

APPENDIX 2: GOVERNMENT DEPARTMENTS AND CONTACTS

A range of Australian Government agencies support the university sector by providing services, guidance, advice and assistance. They do so in areas including international education, higher education, national security, protective security and regulatory matters. This following summarises some of the agencies and departments.

National Counter Foreign Interference Coordinator

The National Counter Foreign Interference Coordinator coordinates Australia's whole-of-government efforts to respond to acts of foreign interference by:

- engaging with the Australian National Intelligence Community in developing assessments of the threat, vulnerabilities and consequences of foreign interference;
- administering the CFI Strategy, that builds on Australia's existing counter foreign interference efforts across government, to create an integrated and coordinated domestic and international program that responds to foreign interference activities;
- coordinating outreach efforts and advice to sectors and systems at risk from foreign interference; and
- enhancing engagement with culturally and linguistically diverse communities to strengthen their ability to challenge manipulation and coercion from foreign actors.

Website: https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/cfi-coordinator

Department of Education

The Department of Education is responsible for national policies and programs that help Australians access quality early childhood education, school education, higher education, and international education and research.

Higher education and research are critical to build and maintain a responsive workforce and a strong innovation system, with the sector spanning undergraduate education through to senior research academics. A strong higher education sector also underpins the world-class reputation and international performance of Australian universities, attracts international students and researchers to Australia, and forges industry collaboration.

The department supports higher education and research through policies, funding and programs.

The department works with the higher education sector to drive innovation and areas of specialisation across universities, embed fairness and equitable access to university for prospective and current students, and to ensure our universities are financially sustainable and affordable into the long term.

The department also drives the Australian Government's *National Strategy for International Education 2025* and works with domestic and international stakeholders to support the sustainable expansion of Australia's trade in education services. The department fosters international collaboration and partnerships with foreign governments and sector stakeholders, identifies opportunities to expand international education engagement, promotes student and researcher mobility between institutions and facilitates the global exchange of knowledge.

Website: https://www.education.gov.au/

Australian Security Intelligence Organisation

The Business and Government Liaison Unit (BGLU) is the principal interface between the Australian Security Intelligence Organisation (ASIO) and government and industry stakeholders. The BGLU provides information via a number of means including a subscriber-controlled website, ASIO-hosted briefings, face to face engagement and participation in joint government and industry forums. All these mechanisms are aimed at providing risk management decision-makers within government and industry with the most current security intelligence and protective security advice to assist them to:

- recognise and respond to national security threats;
- develop appropriate risk mitigation strategies; and
- provide informed briefings to executives and staff.

The BGLU secure website operates on a free subscription basis. The BGLU website contains intelligence-backed reporting on the domestic and international security environment. This reporting is drawn from the full range of ASIO's information holdings and expertise (including the multi-agency National Threat Assessment Centre, ASIO's protective security area (T4) and the Counter-Espionage and Interference Division) and some foreign intelligence partner agency reports.

Website: https://www.bglu.asio.gov.au/
Phone: (02) 6234 1668
Email: bglu@asio.gov.au

Australian Signals Directorate

The Australian Cyber Security Centre (ACSC), in the Australian Signals Directorate (ASD), is the Australian Government's lead on national cyber security. It brings together cyber security capabilities from across the Australian Government to improve the cyber resilience of the Australian community and support the economic and social prosperity of Australia in the digital age.

The ACSC drives cyber resilience across the whole of the economy, including critical infrastructure and systems of national interest, federal, state and local governments, small and medium business, academia, the not-for-profit sector and the Australian community.

It is the hub for private and public sector collaboration and information-sharing, to prevent and combat cyber security threats and to minimise harm to all Australians.

More specifically, the ACSC:

- responds to cyber security threats and incidents as Australia's computer emergency response team (CERT);
- collaborates with the private and public sector to share information on threats and increase resilience;
- works with governments, industry and the community to increase awareness of cyber security; and
- provides information, advice and assistance to all Australians.

Website: https://www.asd.gov.au/cyber
ReportCyber Website: https://www.cyber.gov.au/report
Email: asd.assist@defence.gov.au
Hotline: 1300 CYBER1 (1300 292 371)

Attorney-General's Department

The Attorney-General's Department's (AGD) purpose is to achieve a just and secure society through the maintenance and improvement of Australia's law, justice, security and integrity frameworks. As of 29 May 2019, AGD is also responsible for industrial relations. AGD delivers programs and policies to maintain and improve Australia's law and justice framework; promote and protect government integrity and transparency; and uphold the rule of law. The department's work is central to the productivity, freedom and wellbeing of all Australians. As part of its security and integrity functions, AGD administers the Protective Security Policy Framework and the Foreign Influence Transparency Scheme.

The **Protective Security Policy Framework** (PSPF) assists Australian Government entities to protect their people, information and assets, at home and overseas.

The PSPF articulates government protective security policy and provides guidance for all entities to support the effective implementation of the policy across the areas of security governance, personnel security, physical security and information security. While the PSPF is mandatory for certain government entities, its principles and guidance represent better practice for all agencies and organisations.

The PSPF is applied through a security risk management approach, with a focus on fostering a positive culture of security within the entity and across the government. Entities realise the PSPF's outcomes by considering the framework's guidance and using security measures proportionately to address their unique security risk environments. This allows entities to apply the PSPF in a way that best suits their individual security goals and objectives, risk and threat environment, risk tolerance and security capability.

Website: https://www.protectivesecurity.gov.au/
Enquiry Form: https://www.protectivesecurity.gov.au/Pages/Contact.aspx

The **Foreign Influence Transparency Scheme** commenced on 10 December 2018. Its purpose is to provide the public and government decision-makers with visibility of the nature, level and extent of foreign influence on Australia's government and political process.

The scheme introduces registration obligations for persons and entities who have arrangements with, and undertake certain activities on behalf of, foreign principals. Whether a person or entity is required to register will depend on who the foreign principal is, the nature of the activities undertaken, the purpose for which the activities are undertaken, and in some cases, whether the person has held a senior public position in Australia.

Website: https://www.ag.gov.au/transparency
Public register: https://transparency.ag.gov.au/
Phone: 02 6141 3222 (Foreign Influence Transparency Scheme helpline)
Email: transparency@ag.gov.au

Department of Defence

Defence Export Controls (DEC) in the Department of Defence is responsible to the Minister for Defence for regulating the export of defence and strategic goods and technologies.

These goods and technologies include:

- military items designed or adapted for military purposes or those that are inherently lethal, incapacitating or destructive; and
- commercial items and technologies that may be used or adapted for use in a military program or contribute to the development and production of chemical, biological or nuclear weapons systems.

Australia's export controls enable the export of defence and strategic goods and technology where it is consistent with Australia's national interests and international obligations.

Website: https://www.defence.gov.au/ExportControls/
Phone: 1800 661066
Email: ExportControls@defence.gov.au

Department of Industry, Innovation and Science

The Department of Industry, Innovation and Science (DIIS) plays a central role in promoting a globally integrated, digital and technology-driven economy.

Its focus is on helping Australian industry, business, and research institutions navigate market disruptions and seek new opportunities, including those presented by digital transformation.

This support leads to the growth of globally competitive businesses to support job creation and a strong and secure economy

DIIS also invests in and supports scientific research, infrastructure, skills development, collaboration and engagement that underpins new discoveries. The portfolio supports research agencies to ensure they are well positioned to undertake high-quality research for Australia.

In addition to administering a range of competitive grant programs, under the Global Innovation Strategy, aimed at helping Australia's innovative entrepreneurs and researchers to collaborate and utilise international opportunities, DIIS provides additional resources to aid their efforts.

Of particular interest is the factsheet '*A guide to undertaking international collaboration*', providing a high-level summary of key challenges and strategies Australian researchers and institutions should consider when pursuing international collaboration. The factsheet also contains a series of links to additional support available from the Australian Government.

Website: https://www.industry.gov.au/strategies-for-the-future/increasing-international-collaboration

The Department is also responsible for policy relating to the Cooperative Research Centres Program, which links researchers with industry to focus on research and development towards use and commercialisation.

Website: https://www.business.gov.au/assistance/cooperative-research-centres-programme

Business.gov.au provides services from across government to support your business. The website connects to information, grants, registrations and support to help your business succeed in Australia.

Website: https://www.business.gov.au
Risk management: https://www.business.gov.au/Risk-management
Phone: 13 28 46

APPENDIX 3: CASE STUDIES

The following case studies are provided to guide decision-makers.

It should be noted that in both cases, there were initial concerns of the risk of foreign interference. The case studies provided are not indicative of the level of due diligence required in each and every interaction the university undertakes. Rather, the case studies demonstrate enhanced due diligence considerations undertaken by the university proportionate to the risk.

CASE STUDY 1

An Australian university (the university) was approached by an intermediary to join a research commercialisation collaboration with a foreign entity. The entity described itself as a civilian and commercially-oriented organisation for engineers (the professional organisation). Representatives of the professional organization then contacted a senior university staff member during an international visit with a public invitation to immediately sign an initial collaboration agreement.

The university referred the proposal to a risk advisory firm for enhanced due diligence for several reasons:

- the technology in question had potential dual-use applications; and
- the professional organisation was domiciled in a nation that does not rank highly on transparency or democracy indices (the foreign nation).

The results of the enhanced due diligence inquiries showed that:

- the professional organisation was publicly endorsed by a scientist who was decorated for his contribution to advanced weapons systems in the foreign nation;
- each of the leaders of the professional organisation simultaneously held roles in the foreign nation's defence/military technology industries; and
- several of those leaders held roles in an entity involved in the development of nuclear weapons for the foreign nation.

The university resolved not to pursue the research opportunity due to a risk that the technology in question might be used to advance the design or development of nuclear weapons in the foreign nation and compromise Australian national security.

CASE STUDY 2

An Australian university (the Australian university) was referred by Australian State Government officials seeking to encourage economic investment to a foreign venture capital fund (the VC fund) as the potential funder of planned campus development works. The name of the fund and the location of meetings implied that the VC fund was controlled by a prestigious international university (the foreign university).

The Australian university referred the proposal to a risk advisory firm for enhanced due diligence for several reasons:

- representatives of the VC fund did not provide adequate information to identify the fund and its precise corporate structure, personnel and investment strategies;
- the foreign university had multiple investment arms and holdings under numerous names;
- the foreign university presented a draft agreement for the Australian university to sign which listed the name and address of the foreign university but was signed by the Vice-President of a separate investment holding; and
- the VC fund was domiciled in a nation that does not rank highly on transparency or democracy indices (the foreign nation).

The results of the enhanced due diligence inquiries showed that:

- the corporate structure, multiple aliases and address of the VC fund could not be categorically ascertained through publicly available sources; and
- the VC fund may have been controlled by a foreign government research institute which purports to focus on the integration of civil and military technology.

The Australian university resolved not to pursue the funding arrangement due to a lack of transparency.

APPENDIX 4: SCENARIO

The following scenario is provided to guide decision makers:

How would a staff member manage a potential security incident?

A staff member is concerned that a research relationship with a foreign company is being used as a front to gain access to university information. The staff member believes this company is using its access to seek information that may be useful to their Government. The staff member is not sure what this includes but the company seems to be repeatedly demanding access to databases beyond their need-to-know and the scope of their contractual agreement. While the staff member has denied the company's requests, they are concerned the company may use what access it does have as a springboard to access more sensitive information.

How should the staff member raise their concerns? Universities will need to consider:

- How security incident reporting work within current structures?
- Which person or group will have ultimate oversight of the reporting?
- How will the Commonwealth be informed about any serious concerns?
- What safeguards are in place to stop any improper access by the company?

In this scenario, the staff member recognised behaviours of concern. Educating staff on these behaviours is essential as staff will often encounter these behaviours first and are best placed to identify and mitigate risk. Universities need to equip their staff with an awareness of:

- What foreign interference is
- The types of behaviours that should be reported
- How to raise concerns about foreign interference
- The risks to people, information and assets that universities may face, and
- Any previous security incidents and lessons learned.

If the staff member's suspicions are confirmed, the university will need to evaluate how this incident unfolded and any lessons learnt in the incident reporting and mitigation processes. Administrative procedures on the process of entering into the relationship, the risks that were not initially identified, the modus operandi of the company and whether, as a result of this incident, other relationships may now be compromised, also warrant examination. An established evaluation process to identify ongoing vulnerabilities is useful.

Embedded processes, robust reporting arrangements, continual education of staff, communications on security awareness, and a model of ongoing evaluation ensures foreign interference risk are managed diligently.

APPENDIX 5: 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, managing sensitivities executive responsible and accountable for the security of people, information and assets to counter foreign interference.
Culture	Authentic consensus and understanding from an intended audience on why it is important to adhere to certain procedures and values.
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 safety 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.

Foreign Influence Transparency Scheme	The Foreign Influence Transparency Scheme, established under the *Foreign Influence Transparency Scheme Act 2018*, is designed to provide the public and government decision makers with visibility over the nature and extent of foreign influence on Australia's federal political and government decision-making processes. This is achieved through the publication of details of these arrangements on a publically-available register at https://transparency.gov.au.
Information Security Management	ISO 27001 standards for Information Security Management Systems (ISMS).
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	ISO 31000:2018 defines "Risk" as the effect of uncertainty on objectives.
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 can imagine. Successful threat modelling requires identifying potential threats, analysing the possible effects of those threats, and determining if the threat is significant and requires a neutralization strategy.

APPENDIX 6: ACRONYMS

ACSC	Australian Cyber Security Centre
AGD	Attorney-General's Department
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
BGLU	Business and Government Liaison Unit
CFI	Counter Foreign Interference
CoI	Conflict of Interest
DIIS	Department of Industry, Innovation and Science
DTCA	*Defence Trade Controls Act 2012*
HDR	Higher Degree Research
ICT	Information and Communications Technology
ISM	Information Security Manual
IT	Information Technology
MoU	Memorandum of Understanding
NZ	New Zealand
PSPF	Protective Security Policy Framework
Taskforce	University Foreign Interference Taskforce
UK	United Kingdom
USB	Universal Serial Bus

APPENDIX 7: RESOURCES AND GUIDANCE MATERIALS

Minister for Education press release – Establishment of a University Foreign Interference Taskforce: https://www.education.gov.au/news/establishment-university-foreign-interference-taskforce

Australia's Counter Foreign Interference Strategy: https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/cfi-strategy

National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018: https://www.legislation.gov.au/Details/C2018A00067

Australian Government Information Security Manual: https://www.cyber.gov.au/sites/default/files/2019-08/Australian%20Government%20Information%20Security%20Manual%20%28August%202019%29.pdf

Essential Eight to ISM mapping: https://www.cyber.gov.au/sites/default/files/2019-07/PROTECT%20-%20Essential%20Eight%20to%20ISM%20Mapping%20%28July%202019%29.pdf

Travelling Overseas with Electronic Devices: https://www.cyber.gov.au/publications/travelling-overseas-with-electronic-devices

Protect your organisation from phishing: https://www.cyber.gov.au/advice/phishing

Cloud Computing Security for Tenants: https://www.cyber.gov.au/publications/cloud-computing-security-for-tenants

Defence Trade Controls Act 2012: https://www.defence.gov.au/ExportControls/DTC.asp

Foreign Influence Transparency Scheme: https://www.ag.gov.au/Integrity/foreign-influence-transparency-scheme/Pages/Resources.aspx

Australian Code for the Responsible Conduct of Research (2018): https://www.nhmrc.gov.au/about-us/publications/australian-code-responsible-conduct-research-2018

National Principles of Intellectual Property Management for Publicly Funded Research: https://www.arc.gov.au/policies-strategies/policy/national-principles-intellectual-property-management-publicly-funded-researches

Australian Research Council Intellectual Property Policy: https://www.arc.gov.au/policies-strategies/policy/intellectual-property-policy

ASIO Business and Government Liaison Unit: https://www.bglu.asio.gov.au/

Australian Government Security Vetting Agency – Gold Standard Proof of Identity: https://www.defence.gov.au/AGSVA/resources/gold-standard-proof-identity.pdf

Protective Security Policy Framework – fact sheets and publications: https://www.protectivesecurity.gov.au/resources/Pages/PSPF-fact-sheets-and-publications.aspx

Medicines Australia – Code of Conduct: https://medicinesaustralia.com.au/code-of-conduct/

Security awareness campaigns – UK Centre for the Protection of National Infrastructure: https://www.cpni.gov.uk/security-awareness-campaigns

Security Considerations Assessment - UK Centre for the Protection of National Infrastructure: https://www.cpni.gov.uk/system/files/documents/04/71/Security_Considerations_Assessment_v4_2019-06.pdf

Security planning – NZ Protective security requirements: https://www.protectivesecurity.govt.nz/security-planning/