Countering foreign interference

Background: Guidelines to Counter Foreign Interference in the Australian University Sector

In 2019 the University Foreign Interference Taskforce (UFIT) was established by the Australian Government to bring together universities and Australian government agencies to develop a set of best practice guidelines to help universities manage foreign interference risks and strengthen resilience against foreign interference.

The Guidelines to Counter Foreign Interference in the Australian University Sector (the **Guidelines**, also known as the UFIT Guidelines), developed in extensive consultation between the Government and the university sector, were released in November 2019, and were refreshed in 2021.

The Guidelines are designed to build on risk management policies and security practices already implemented by Australian universities, as well as assist decision makers to assess the risks from foreign interference. They recognise that universities have different risk profiles and encourage universities to adopt measures to mitigate foreign interference risks that are appropriate to their particular risks, and support universities to develop new, or examine existing tools, frameworks and resources to assess and mitigate risks from foreign interference.

The overarching principles that were applied when developing and refreshing the Guidelines are as follows:

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

As stated in the Guidelines, a proactive approach by the university sector to the threat of foreign interference will help 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.

The Guidelines "seek to strike a balance and give careful consideration to the potential tensions between developing institutional policies that protect against the risk of foreign interference, while also promoting the free exchange of ideas, an open research culture and academic freedom" (page 5), and are organised into key themes or pillars, each with set objectives to guide universities, including governance and risk frameworks; due diligence; communication, education and knowledge sharing; and cybersecurity.

What is foreign interference?

When considering our obligations with respect to safeguarding against foreign interference, it is important to distinguish between *foreign interference* and *foreign influence*. The Guidelines define these as follows:

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

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

Examples of foreign interference include:

- improper attempts to obtain sensitive or confidential information from students or staff (e.g. via foreign delegations, seminars, collaborations, or in return for financial support)
- inappropriate targeting and recruiting staff and students, to further a foreign actor's interests
- actions by or for a foreign actor that are inconsistent with academic freedom and the university's values and codes of conduct, such as demands or inducements to change academic programs for the benefit of a foreign political, religious or social agenda
- inappropriate efforts to alter or direct the university's research agenda into particular areas of research (this may occur through subtle forms of undue influence and engagement, and through funding arrangements that may also lead to a loss of future value and/or control of intellectual property)
- seeking inappropriate access to, or influence over, particular persons, areas of activity, or research outcomes through various forms of funding arrangements (e.g. donations) or collaborations, financial or other inducements targeted at individuals; and
- cyber targeting by exploiting network vulnerabilities and unauthorised access.

What are the risks to the university foreign interference?

Risks of foreign interference include:

- compromise or unauthorised access to valuable university research, sensitive or personal data;
- damage to the reputation of the university or its research teams and individual staff and students;
- loss of future partnerships and collaborations or opportunities to attract talent;
- breach of legal obligations (contractual or legislative);
- foreign governments gaining an undue commercial, technical or intellectual advantage to the disadvantage of the university;
- loss of intellectual property and commercialisation opportunities;
- cultivation of the university community for information gathering and espionage against Australia;
- undue influence of an agenda within or outside the classroom.

What are the responsibilities of the university, and staff and students (in particular HDR students) with respect to countering foreign interference?

The key pillars and the related objectives set out in the Guidelines should be considered by universities proportionate to their risk. Those pillars, the set objectives, and the key responsibilities of all university staff with respect to the key pillars, are as follows:

1. **Governance and risk frameworks:** Among other things, universities should have frameworks for managing their risks that address foreign interference threats to their people, information and assets; accountable authorities responsible for managing foreign interference risk; and policies and procedures that set out responsibilities and expected conduct to manage foreign interference risk.

Charles Sturt staff and students should:

- have regard to guidance and oversight provided by the Deputy Vice Chancellor Research, who is the university's accountable authority (Note: further work is in progress to clarify responsibility for reporting and resolving concerns related to foreign interference);
- consult the Legislative Compliance Guide for details of material compliance obligations related to foreign interference, the executive responsible for compliance, the compliance coordinator, and the business units impacted;
- have regard to applicable policies and procedures that refer to the need to take care when considering arrangements to identify, manage and report any risks of foreign interference (Note: our policies are currently under review with a view to providing clearer guidance with respect to procedures for identifying, managing and reporting instances of foreign interference);
- understand that if anyone is aware of or reasonably suspects that foreign interference is occurring in relation to university activities, they must report it immediately to an appropriate officer (Note: as policies and procedures for identifying, managing and reporting instances of foreign interference are still being developed, any reports of suspected foreign interference should in the meantime be notified immediately to the Office of the Deputy Vice Chancellor Research and to Legal Services).

Please refer to section 4 (cybersecurity) for additional guidance on risks related to cybersecurity, including procedures for protecting USB drives from risks.

2. **Communication, education and knowledge sharing**: Universities should have communication plans and education programs that raise awareness and support mitigation of their foreign interference risks; provide training to staff and students who are engaged in foreign collaboration or other partnership activities at risk of foreign interference; and should participate in sector-wide counter foreign interference events and where appropriate, share experiences and leading practice, to learn from each other and build sector resilience.

Charles Sturt staff and students should:

- be aware of known and emerging risk factors across the higher education sector relating to foreign interference;
- be aware of information issued by government agencies and advisory services and recognise common issues and threats;
- be aware of and seek guidance on how to deal with undue foreign interference;
- participate in sector-wide counter foreign interference events where appropriate to their role and responsibilities;
- communicate with colleagues and peers about strategies for managing foreign interference risks, even when those risks may be considered low;

- assist in educating colleagues, especially early career researchers and HDR students, about foreign interference risks.

3. **Due diligence, risk assessments and management**: Universities should require declaration of interest disclosures from staff who are at risk of foreign interference, including identification of foreign affiliations, relationships and financial interests; conduct due diligence to inform decision-makers of foreign interference risks; conduct due diligence on partners and personnel; assess the potential of technology and/or research; apply a comprehensive approach to their due diligence; and have appropriate approval, audit and continuous evaluation of due diligence processes.

Charles Sturt staff and students should:

- know the partners our respective business units engage with or whom we collaborate with;
- be aware of risk factors relating to foreign interference, particularly if proposed activities involve sensitive research, dual-use technologies or valuable intellectual property;
- in the case of staff, conduct necessary due diligence before committing to arrangements with third parties (Note: guidance on how due diligence is to be conducted and which parties and research partnerships should undergo due diligence reviews is under development. In the meantime, anyone engaging in any activity or partnership on behalf of or with a foreign government, foreign university, foreign business or any other foreign organisation or entity as part of their university business must evaluate the proposed activity or partnership for the risk of foreign interference, foreign influence and/or statutory reporting or regulatory obligations, and should seek assistance from the head of their business unit and/or the Office of the Deputy Vice Chancellor Research, as appropriate);
- when undertaking due diligence with respect to any material arrangements with third parties, identify foreign ownership relationships and record these details on an appropriate register;
- if a risk of foreign interference is identified in relation to any university business activity or collaboration, notify the Office of the Deputy Vice Chancellor Research and Legal Services immediately. The Office of the Deputy Vice Chancellor Research, in consultation with Legal Services and other appropriate advisers, will assess the risk and consider what, if any, mitigation measures may be required in connection with the proposed partner and activity as proportionate to the risk. Measures to mitigate the risk of foreign interference might include:
  - requesting further due diligence of the activity or partner
  - seeking further/stricter contractual protections
  - a recommendation to reconsider engaging in the activity or with the partner
  - other actions appropriate to the risk (including, where appropriate, escalation to senior leadership and a possible recommendation that the university not proceed with the proposed arrangement)
- comply with university policies and procedures related to conflicts of interest, and obtain declaration of interest disclosures from staff (and, where appropriate, students engaged in research collaboration) who are at risk of foreign interference, including identification of foreign affiliations, relationships and financial interests;
- consider whether specific arrangements meet the legislative criteria for notification as set out in Foreign Arrangements Scheme (under the Foreign Arrangements Scheme established by the *Australia's Foreign Relations (State and Territory Arrangements) Act 2020*, universities are obligated to notify the Minister of Foreign Affairs if they propose

to negotiate or enter an arrangement with a foreign government or foreign university that lacks institutional autonomy to ensure that such arrangements do not adversely affect Australia's foreign relations and are not inconsistent with Australia's foreign policy).

4. **Cybersecurity**: Universities should understand and proportionately mitigate cyber business risks, using techniques like threat models where possible, to inform their cybersecurity strategy; implement a cybersecurity strategy that treats cybersecurity as a whole-of-organisation human issue and incorporates an appropriate controls framework; and participate in communities of best practice, which share cyber intelligence and lessons across the sector and government.

Our Division of Information Technology has established a cyber security program which:

- ensures ongoing enhancement of the university's capability and control environment;
- has introduced additional preventative controls; and
- has engaged external subject matter experts who, in conjunction with DIT personnel, continue to support the management of cybersecurity and foreign interference risks.

Charles Sturt staff and students should:

- be aware of and understand the potential cybersecurity threats relevant to their activities and cultivate protective behaviours across the university;
- comply with guidance provided by DIT with regards to cybersecurity risks and controls;
- notify DIT immediately whenever cybersecurity threats are identified or suspected; and
- participate in communities and events which consider cybersecurity risks and best practice responses, where appropriate to their role and responsibilities.

Risks related to USB drives

All staff and students, especially researchers and HDR students, are reminded to be vigilant in respect of cybersecurity risks, especially when attending conferences and receiving items in the mail, as you may be approached or receive items (in particular USB sticks/drives etc) which could lead to malware being installed on your devices and the university's systems (without your knowledge).

Likewise, your USB drives can contain sensitive information (valuable, confidential and/or personal information) which needs to be protected. Protecting data on USB drives can be achieved by the following simple steps:
- Ensure the physical safety of your USB drives
- Do not plug unknown USB drives into your computer
- Use secure USB drives for sensitive information when appropriate and possible (e.g. models with fingerprint authentication)
- Use USB drives from reputable sources (do not purchase from unverified suppliers and do not use USB drives handed out at conferences or received from unknown/unverified sources)
- Keep your computer software and anti-virus up to date (this helps protect against malware)
- Delete files from USB drives that are no longer required
- Use encryption.

Further updates:

Charles Sturt's responses to the Guidelines and each of the key pillars/themes are continuing to evolve, and are also being informed by additional guidance and recommendations arising from the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) Inquiry into national security risks affecting the Australian higher education and research sector, which was handed down in March 2022. The PJCIS report findings detailed a number of issues concerning national security, including foreign interference, cyber risks, espionage, and undisclosed foreign influence; and set out a series of recommendations to address national security risks the sector is exposed to.

An online ELMO training module related to foreign interference is under development and should be available by the end of 2022.

In the meantime, please continue to monitor university communications, changes to policies and procedures, and information from the Office of the DVCR or your business unit, for further guidance about the university's response to foreign interference risks.