Appendix 3: Measures taken by the Go8 to mitigate the threat of foreign interference in alignment with the UFIT Guidelines

Governance and Risk Frameworks

Australian National University (ANU)

- Has created the **Foreign Interference Advisory Committee (FIAC)** which is chaired by the Deputy Vice-Chancellor (Research and Innovation) and includes two Vice-Presidents, two Deans and the Chief Information Security Officer. The FIAC reports to the University Research Council. It uses a risk assessment matrix to determine the risk of any given international engagement, gift, or appointment. These assessments are maintained by the FIAC secretariat and form the basis of future reporting. Reporting on foreign interference is also provided to the Audit and Risk Management Committee as well as Council on a regular basis.
- Foreign interference is to be added, along with all other information security risks, to the enterprise risk register in 2021, however foreign interference is already a risk assessment point with the research services division and more recently International Strategy and Partnerships. These areas work closely with the Information Security Office to risk assess research agreements and appointments which are then reported to FIAC. Formal policies and risk management frameworks pertaining to foreign interference and other information security risks is due for implementation in 2021.
- University procedures already require notification of international collaborations and appointments. However, a full process review was undertaken in 2020 to identify areas in which improvements can be made. Notably this includes points in the process chain where intelligence led risk assessments can be added to ensure ANU does not engage, unknowingly, with entities of concern. As above, a full policy review of all information security polices will be undertaken in 2021.
- The FIAC uses a risk assessment matrix to determine the risk of any given international engagement, gift, or appointment. These assessments are maintained by the FIAC secretariat and form the basis of future reporting. Reporting foreign interference is also provided to the Audit and Risk Management Committee as well as Council on a regular basis.
- Research Services Division and International Strategy and Partnerships form the primary basis of information capture and reporting of all foreign interactions. They escalate, as required to the FIAC and the Information Security Office when additional due diligence is required. All assessments are kept by the FIAC secretariat. Reporting on foreign interference is also provided to the Audit and Risk Management Committee as well as Council on a regular basis.
- ANU has recently introduced a Conflict of Interest (COI) declaration process for foreign affiliations etc. Once policies are reviewed in 2021, ANU will establish a statement of commitments in line with these policies.
- Regular feedback is provided to the FIAC and review of the information security capability which includes foreign interference, will be undertaken in 2021 and a full audit scheduled in 2022.

University of Adelaide

- Convened by the Deputy Vice-Chancellor (Research) and chaired by the Chief Security Officer (CSO), the **Defence & Security Committee (DSC)** has been established with representation from Information Technology and Digital Services, Legal and Risk, Innovation and Commercial Partnerships, Research Services, the Industry Engagement Priorities, the Research Institutes,

Human Resources, Global Engagement and the Adelaide Graduate Centre. The DSC is established to:

i. Assist the CSO with the development and implementation of new and revised policies and procedures, training programs, risk management frameworks and performance monitoring processes, aimed at ensuring that the appropriate security standards required for broad Government and Defence collaborative activities are met at all levels of the University.

ii. Assist with embedding relevant information about national security vulnerabilities, reporting pathways and risk mitigation measures into existing University policies, procedures and guidelines.

iii. Coordinate the monitoring and assessment of whole-of-University compliance risk to ensure the University meets its obligations in relation to defence, national security, the FITS Act and UFIT guidelines.

- A subcommittee of the DSC, the **National Security Compliance and Reputation Risk Assessment Committee (NSCR-RAC)** is to be established to review foreign engagement activity that, whilst legally compliant to the various legislative obligations, has been flagged as requiring broader evaluation from a reputational risk perspective.

University of Melbourne

- Oversight of the implementation of the University Foreign Interference Transparency (UFIT) Guidelines has been led by the **Foreign Interference Working Group**, a sub-committee of the University's existing **Research Due Diligence Advisory Group**.
- Members of this Working Group are senior University representatives from Legal and Risk, Research Innovation and Commercialisation, Information Technology, Human Resources, Chancellery International, Advancement, and Chancellery Research and Enterprise.
- The Working Group has oversight of the implementation of the UFIT Guidelines and the University of Melbourne is well advanced in progressing a staged UFIT Action and Implementation Plan.
- Additionally, several other working groups and committees drawing on senior leadership across University areas are being or have been established to ensure oversight and risk management is comprehensive and responsive.
- An environmental scan and gap analysis led by the Deputy Vice-Chancellor (Research) identified many existing mechanisms, processes and protections already in place within the University, as well as areas that needed strengthening.

Monash University

- Monash has established a **Transparency and Integrity Committee (TIC).** This reports to the Vice-Chancellor's Group (the University's core leadership team) and monitors Monash's overall framework to counter potential foreign interference to ensure an integrated, cross-organisational approach, as well as reviewing projects with higher risk exposure to foreign interference risk. It is supported by working groups to support consultation across the university and implementation of change as required.
- The **University Council and Audit and Risk subcommittee** of Council are also regularly briefed on projects with higher risk exposure to foreign interference risks and through routine contractual and financial delegations' processes. The Audit and Risk subcommittee has responsibility for providing advice to the Council in the areas of internal control and strategic risk.

- With effect from 1 July 2020, Monash University brought risk and governance functions under a single portfolio led by the Deputy Vice-Chancellor and Senior Vice-President (Enterprise and Governance), who leads institutional governance coordination on foreign interference.
- As part of governance reforms to Monash University's wholly owned pathway provider, Monash College, all international arrangements proposed by the College are now reviewed and approved at University level ensuring one lens is applied to foreign interference risks that may arise in the course of the College's international work.
- Monash University's Conflict of Interest (COI) procedure applies to paid staff, adjuncts and honorary appointments. It requires individuals to declare any potential, perceived or actual conflict of interest if one arises, together with a management plan. All new staff are required to complete several mandatory training modules, including one on COIs. Current staff are required to repeat the training every 3 years.
- Monash University's Paid Outside Work procedure applies to all paid and unpaid staff and requires staff to apply to undertake any paid work outside of the University, as well as declare roles where there may be a conflict with their University adjunct role.
- In cases of conflict of interest where the conduct can be classified as misconduct or serious misconduct, the matter will be referred for consideration under the University's staff disciplinary procedures.
- Policy review and development is underway for several 'principal' policy documents that will further strengthen the University's approach to foreign interference. These include policies covering Anti-Fraud and Corruption, International Partnership agreements, Conflict of Interest, Paid Outside Work, Responsible Conduct of Research, Sanctions and Export Controls, Gifts and Graduate Research Student Supervision.
- Risk assessments are undertaken for major initiatives. Risk assessment occurs at different phases of an initiative/project (from proposal to project establishment) with oversight and monitoring of risks by Steering and Executive Committees.
- Each of Monash's 10 faculties has a Deputy Dean, Associate Dean (International) or equivalent who has a broad remit to support the Faculty Dean on leading each faculty's engagement with international matters. The responsibilities of this role have been strengthened to ensure there is faculty-level coverage, awareness, and oversight of foreign interference risks.

University of Sydney

- The University's Executive has adopted an integrated institution-wide **Foreign Interference Coordination Framework and Work Program** for 2020, overseen by the University's Senior Deputy Vice-Chancellor and supported by staff in the Vice-Chancellor's Office and lawyers from the University's Office of General Counsel.
- Policies and processes have been developed and implemented with a set of clear principles to guide University decision makers, staff, affiliates, and research students when considering engaging in collaborations with foreign entities or individuals.
- Establishment of a **Research Risk Advisory Committee** to consider and advise decision-makers on foreign interference and national security concerns arising from research-related activities.
- Establishment of a **Research Risk Operations Group** to identify, discuss and review relevant strategic issues and provide advice to the Research Risk Advisory Committee and via its members to Faculties, University Schools and Centres and their research committees.

- Appointment of a **Manager, National Security and Export Controls** within the Research Portfolio to implement policy and processes across the University for defence trade controls and prohibited exports, and to ensure staff engagement with relevant laws and guidelines.

- Development and roll-out of face-to-face and online training for staff in high-risk disciplines about national security laws and guidelines, relevant university policies, processes, and support services.

- The creation and maintenance of a **University UFIT Guidelines Compliance Matrix**, mapping the University's relevant activities to the guidelines and tracking the progress and outcomes achieved as projects are implemented.

- The establishment of a secure online site, which houses the **Matrix**, other relevant resources and provides a protected forum for relevant staff communication.

- The establishment of a **University National Security Network** comprising academic and professional staff with relevant responsibilities, to share information, updates, and coordinate activities in response to relevant developments.

UNSW Sydney

- UNSW has established a working group to consider the breadth of the UFIT Guidelines (UFIG) and to provide recommendations as to how UNSW should ensure it meets its obligations. The objective of the working party is to generate an overarching **Foreign Interference Framework** that will outline:

    1. How UNSW's suite of current policies, procedures and practices integrates foreign interference exposure considerations and adopts best practice.
    2. How UNSW will maintain awareness and capability to assess and manage foreign interference matters.
    3. How UNSW will report foreign interference matters and manage incidents, including any Defence Industry Security Program (DISP) reporting requirements.
    4. How foreign interference requirements will be addressed as part of the DISP accreditation process.

- A key deliverable of the working party is to map UFIG considerations against relevant UNSW's policies, procedures and practices (e.g. Conflicts of Interest). An outline of this mapping exercise was provided as part of the update to Universities Australia in May 2020 and has formed the basis of the University's current discovery activity. The tasks currently being undertaken include:

    - Identification of the reporting requirements (whether BAU or incident based), forums and frequency
    - Integration of UFIG considerations into the following:
        - Procurement policy and procedure
        - Approach to third-party engagements, including counterparty due diligence, approval processes (e.g. industry research approvals), contractual agreements
        - Gifts and sponsorships policies and guidelines
        - Conflicts of Interest Policy and Procedure

        - Staff and Research Codes of Conduct
        - Recruitment
        - Reporting Wrongdoing and Fraud Prevention Frameworks
        - Risk Management Framework
        - Data & Information Management
        - Data and Security Management
        - Cyber Security Framework
    - Development of a government liaison engagement and communications strategy to assist in the sharing of information with agencies such as ASIO, DFAT, Defence Security and Vetting Service, etc.
    - Development and implementation of a training program that leverages existing training where possible and integrates training requirements into job specifications
    - Contribute to the ongoing maturity of the University Sector's response to foreign interference
    - Ensure third line review of controls by internal audit once established.

University of Queensland

- UQ maps carefully its adherence to the Guidelines and, prior to the Guidelines being released, UQ commenced work on a number of actions to address the key themes and objectives of the Guidelines in its operations as outlined below.
- UQ has taken a number of proactive steps to identify and respond to the potential threats of foreign interference highlighted by the Guidelines, including implementing three key control measures:
    - Implementation of four disclosure tools, which require disclosure and management of conflicts of interest, secondary employment, sensitive research and foreign influence.
    - Improvements to its existing defence export controls and sanctions compliance system.
    - Development of a comprehensive cyber-security strategy.
- These measures are in addition to UQ's comprehensive enterprise risk and compliance program and other controls to manage foreign interference risks. Details on these measures are described below.
- In addition, UQ has established a Foreign Influence Task Force, chaired by the Provost, which reports to the University Senior Executive Committee. This group is charged with identifying and addressing the risks and issues around foreign influence. The group also oversees and monitors the compliance with the suite of disclosure tools referred to above.

- **Disclosure Tools**: UQ is not solely relying on policies and procedures (although they are essential) and has developed a series of tools that require staff to interact with key issues.
    - Over the past three years, UQ has undertaken a systematic and comprehensive program of work to provide a new policy and operational framework to understand whether staff have any interests, hold any additional positions or undertake any research activities in sensitive areas which might give rise to conflicts of interest or commitment. This foundational work

has enabled UQ to address the related challenges arising from foreign interference, foreign influence or associated national security risks.

- Through these tools, which have been live since 15 May 2020, UQ has required all staff to disclose their interests (on an annual basis or as circumstances change), activities and positions (including any foreign talent recruitment positions) in accordance with the Conflict of Interest Policy in relation to the following areas:
  - Conflicts of interest disclosure tool in accordance with the Conflict of Interest for Members of Staff Policy and Procedure. All staff must complete this online tool.
  - Secondary Employment Register in accordance with the Consultancy, Secondary Employment and Internal Work Policy. All academic staff and HEW 8 and above must complete this online tool.
  - Sensitive Research Register. All academic staff must complete this tool.
  - Foreign Influence Disclosure in accordance with the Foreign Influence Disclosure Procedure. All academic staff and select senior professional staff must complete this online tool.

- These registers, and the associated policies and procedures, perform several functions which achieve the key objectives under the UFIT Guidelines including:
  - Raises leaders and staff awareness of and be clear on the risks with staff relating to foreign interference, foreign influence, data theft and espionage;
  - Educates staff on specific aspects of their obligations through FAQs in the registers;
  - Provides both 'line of sight' for managers/supervisors and a definitive source of baseline data of UQ activity, not relying on other corporate systems;
  - Enables more effective training to be targeted to specific cohorts of staff from external experts and the UQ Office of Research Ethics and Integrity;
  - Enables comprehensive reporting to line-managers and Senior Executives on UQ activity;
  - Enables workflows to line managers for approvals where required; and
  - Enables management of these risks under the UQ Enterprise Risk Management Framework.
- Comprehensive reports are available to line managers and heads of organisational units. The heads of organisational units reviewed the disclosures and took follow up action to ensure that the disclosures were completed by all relevant staff. As at the date of this submission, the completion rate is more than 95%.
- Information from the disclosure tools is enabling UQ to have greater oversight of any potential risks to Australia's national security, including:
  - Second appointments must be disclosed for approval. Approval is only granted by UQ contingent on partner organisation suitability, sensitive research considerations, protection of intellectual property (IP) arrangements, and overall benefit to UQ (as representative of the Public Interest).
  - Collaborations with foreign organisations must be disclosed when involving sensitive research areas.
  - Private business interests must be disclosed, and commercialisation of University IP must not involve a conflict of interest with private financial interests.

UQ's Enterprise Risk and Compliance Program

- In addition to the specific controls identified above, UQ has a comprehensive enterprise risk and compliance program that supports the management of foreign interference risks and associated national security risks. This program includes:

(a) institutional governance through the Senate, Senate Risk and Audit Committee, Senior Executive Team and Academic Board.

(b) monitoring and assurance environment through cyclical reporting, monitoring and reviewing processes.

(c) governance and risk frameworks through the UQ Governance and Management Framework, Enterprise Risk Management Framework and Enterprise Compliance Management Framework.

(d) the relevant UQ units and teams involved in the management of risks include Enterprise Risk Services (Governance and Risk), Enterprise Compliance Unit (Governance and Risk), Internal Audit, Integrity and Investigations Unit and the use of targeted committees and working groups, such as the International Safeguards Assessment Group.

(e) where a risk is identified, remedial action is taken under the relevant procedures, including the Managing Complaints about the Conduct of Research Procedure, staff misconduct/serious misconduct processes in The University of Queensland Enterprise Agreement 2018-2021, Research Misconduct – Higher Degree by Research Students Procedure and Student Integrity and Misconduct Policy.

University of Western Australia

- UWA assigned a senior staff member full time for three months to conduct an extensive review of national security and foreign interference risks at the University, including the risks highlighted in the UFIT Guidelines, sanctions compliance, and DTCA compliance. The project resulted in a report to UWA's Executive with 28 recommendations. This senior staff member remains responsible for the ongoing development of the University's systems to counter foreign interference.
- UWA then established a Foreign Interference Advisory Committee (FIAC), comprising the University's four Deputy Vice-Chancellors, the Director of Governance and Legal Counsel, and the Chief Digital and Information Officer. FIAC oversees responses to foreign interference issues and prioritises actions to strengthen the University's systems. It has created 2020 and 2021 work plans based on the recommendations of the report mentioned above.
- UWA has created a new Foreign Interference Compliance Officer position to work with a team from each major portfolio to implement these prioritised actions, which include:
    - a program of foreign interference training appropriate to the needs of different parts of the University;
    - work on an expanded register of staff members' external links, affiliations, and employment;
    - the development of nuanced risk management approach to cyber security at UWA, particularly for sensitive research areas;
    - workshops on foreign interference risks and the creation of a risk matrix.

Due Diligence

Australian National University

In addition to the measures outlined under Governance and Risk, above:

- As above, a full policy review of all information security polices will be undertaken in Q1 and Q2 2021, along with outreach and education activities.
- ANU has created a background checking service which is used throughout the enhanced due diligence process to ensure the University knows who their partner is and what the risks may be. This can be initiated via FIAC or by an individual academic.
- FIAC assessment processes take into consideration all relevant legislation including the *Defence Trade Controls Act*, autonomous sanctions legislation, and the *Foreign Influence Transparency Scheme Act 2018*.
- The FIAC maintains a list of all risk assessed collaborations which will be periodically reviewed. Some risker engagements will have additional controls in the form of regular review points as part of a risk mitigation plan.
- ANU has commenced outreach with research school directors in high-risk areas around boosting the capacity of research staff and Higher Degree Research (HDR) students to assess risk in their research projects.
- ANU has created a background checking service which is used throughout the enhanced due diligence process to ensure the University knows who their partner is and what the risks may be. This can be initiated via FIAC or by an individual academic.
- Philanthropy and donations are included in the FIAC process (see above).
- Potential end-use possibilities, dual-use and potentially sensitive technology and research outcomes are all considered under the FIAC process (see above).
- Research Services Division and the Technology Transfer Office oversight the use and transfer of patents. Any high-risk undertakings also involve the information security office.

University of Adelaide

To assist in responding to the objectives of the Guidelines, the University has re-oriented existing capabilities in dealing with complex regulatory requirements and responding to expanding engagement with DST where security and protection of systems and processes is critical. This includes the establishment of the following dedicated positions:

- A Chief Security Officer (CSO) to provide academic leadership and plan for overall achievement of the University's strategic goals by ensuring it complies with essential regulatory requirements and best practice in relation to defence, national security and foreign influence, and interference regulations and guidelines. In February 2020, Professor Bruce Northcote was appointed to this role in a 0.2 FTE capacity, initially for 6 months. Subsequently, recognising the increasing compliance obligations of the University in these areas, in November 2020 his appointment was confirmed full-time to the end of 2022.

- A Senior Defence and National Security Compliance Officer (DSO) responsible for ensuring compliance with export controls regulation (including *Defence Trade Controls Act*, *Autonomous Sanctions Act*), managing the processes designed to ensure that the University meets its requirements of the Defence Industry Security Program, and managing a strategy to ensure the University meets its obligations in relation to foreign influence and interference. This is an expansion of the prior Defence Security Officer position held by Dr Scott Willoughby, who has taken on the enhanced full-time role.
- A Senior Legal Advisor (Research) specialising in the requirements of the Foreign Interference Transparency Scheme (FITS), the UFIT Guidelines, Defence Trade Controls, and International Sanctions. The University has been unable to fill this position (having gone to market). To cover for this the University estimates that 0.3 FTE of other internal legal resource has been diverted *plus* the University has outsourced approximately $55,000 of legal work to date.
- **Foreign Engagement Declarations**: For university staff individually: All personally-arranged foreign appointments (remunerated or otherwise) and/or activity with a foreign entity that results in benefit to the staff member exceeding the Conflict of Interest (CoI) value threshold of $500 is to be declared through the Foreign Engagement Declaration (FED) process. Failure to declare, or failure to be completely transparent about foreign activities could be considered to be misconduct under the University's Enterprise Agreement. The declaration requirement will become integrated into each individual staff member's Planning & Development Review (PDR) process, such that it will be required to be undertaken annually. It is NOT required to register foreign activity that would be considered part of an academic role at the University of Adelaide (unless the CoI benefit threshold is exceeded), such as the following:
    - Fractional appointments at foreign institutions that were known (by UoA HR) prior to employment at UoA.
    - Participation in international conferences and academic journals, including on editorial boards, etc.
    - Informal research collaborations, including international travel by a UoA academic paid for by UoA or academic funds.

    To date 97.7% of non-casual active academic staff (including titleholders and adjuncts) have completed a personal declaration. The entirety of the 2.3% non-compliant cohort are surgeons or clinicians that have been 'difficult' to chase up (almost all are adjuncts). The Office of the CSO is working with academic leadership to evaluate and classify the declarations and determine next steps as follows:
    - "**Red**": A matter about which serious consideration needs to be undertaken regarding possible FITS registration.
    - "**Grey**": An academic appointment that is potentially remunerated (could be similar to a Talent Plan), about which more information needs to be obtained. These then will be reclassified as Red or Yellow.
    - "**Yellow**": A potential Conflict of Interest (often due to a received benefit exceeding the $500 CoI threshold, for example as paid travel expenses) that needs to be registered with the staff member's supervisor with (potentially) a management plan developed.
    - "**Green**" (remainder): Nothing substantive to declare.
- **Foreign Engagement Compliance Reviews**: All university-arranged activity that entails engagement with a foreign entity needs to be registered and approved through the Foreign Engagement Compliance Review (FECR) process PRIOR to it being agreed (formally or informally) with the foreign entity. One faculty has a system in place that requires registration of international

visitors to campus. Registering visitors has not been mandated across the whole university but may be required in future. Since implementing FECR in May 2020 there have been 185 FECR submissions (this is expected to be larger in non-COVID-19 years), 164 of which have been approved to proceed.

University of Melbourne

- The Office of Research Ethics and Integrity (OREI) is the University's main point of contact for issues relating to animal welfare, animal and human ethics, research integrity, research misconduct, gene technology, biosafety, biosecurity, and export controls. Overseen by the Associate Director, Research Governance & Quality, roles such as the Export Controls Officer, the Biosafety and Biosecurity Officer, and the Program Manager Clinical Trials support implementation of the University's framework for managing export controls and sanctions, work to ensure research-related risks are appropriately managed, and that the full circumstances of any proposed research funding are understood before being accepted.
- OREI staff work in close consultation with the University's contracts and grants team, including the Due Diligence Officer, Legal and Risk, and Chancellery Research and Enterprise.
- In 2018, the University undertook a program of work to develop a principles-based framework to guide decisions about undertaking research with external parties. This included a decision-making pathway for determining when particular research and research partnerships present potential risks to the University's research values and reputation, and/or jeopardise the integrity and independence of its research.
- To supplement these principles and ensure robust academic oversight, a strengthened due diligence review process was adopted, as well as the establishment of the Research Due Diligence Advisory Group (RDDAG).
- Chaired by the Deputy Vice-Chancellor (Research), the RDDAG is an oversight and advisory group which provides process review and point of escalation on research due diligence and related risk matters; it considers emerging and potential risks, including any potential or perceived foreign influence, interference and/or security threat risks, at either sector or country level. It brings together key senior stakeholders from across the University from areas such as Legal and Risk, University Council, Academic Board, Government Relations and Academic Divisions. Critically, it has brought together different areas of the institution, such as Research and Advancement, to capture risk-related processes and matters that might arise via a number of avenues so as to ensure a coordinated and whole-of-institution response.
- Initiatives underway in the OREI to optimise sanctions compliance, including formal documentation of an institutional compliance action plan for sanctions; proactive review and targeted outreach to embed sanctions compliance in relevant processes, including to Graduate Researchers and Supervisors; and development of enhanced due diligence mechanisms, including procurement of software to enable multiple sanctions lists to be searched simultaneously.
- In 2020-21, the Research Office will offer 'Know your Partner' due diligence training and the OREI will also continue engagement with the Australian Sanctions Office to offer annual DFAT-conducted sanctions training. The Legal and Risk Unit have developed a general compliance training module that is now available for all staff regarding the *Foreign Influence Transparency Scheme Act 2018* (Cth).

- There are currently two project teams (one staff-related, one student-related) working through a series of recommended actions to improve international travel policy, procedure, process, practice and supports.
- Membership of the University's Research Due Diligence Advisory Group has been extended to include a University Council member who also sits on the University's Gifts Committee to ensure oversight and consideration of donor due diligence that may overlap with research due diligence matters;
- Upskilling University lawyers to review all material contracts in order that they can identify any potential risk for foreign influence and then raise with relevant contract owners to assist with an assessment of foreign influence risks in accordance with the *Foreign Influence Transparency Scheme Act 2018* (Cth).

Monash University

- Monash's **Due Diligence Risk Assessment guidance materials** have been refined to support awareness of foreign interference risks and to ensure consistency across the university.
- Monash has a **Major Opportunities Group (MOG)** which operates as a forum to strengthen the development of large, complex and strategic projects early in their development. As part of the operation of this group, feedback on risk of foreign interference and the requirement for due diligence on any aspect of each project is provided, as relevant. Projects are referred as necessary to the Transparency and Integrity Committee if they are assessed as higher risk. MOG provides advice both to project leads and to the Vice-Chancellor's Group. The Monash Research Office, Risk and Compliance Unit, Office of General Counsel, Deputy Vice-Chancellors, and relevant faculty offices all play a key role in ensuring strong governance.
- As required, Monash draws on expert due diligence undertaken by external advisory firms with detailed knowledge of the legal, financial, regulatory, and corporate structures of the relevant country in support of its international projects and programs.
- The **Monash Research Office (MRO)** works collaboratively across the institution to ensure implications of sanctions laws, defence trade controls and risk of foreign interference are assessed in research projects.
- All proposed philanthropic gifts are subject to appropriate due diligence checks per the **University's Philanthropic Gifts Policy**.
- Monash's **Intellectual Property (IP) Policy and Procedures** confirms the requirement for Monash staff to proactively report disclosures to the University's designated lead officer for IP oversight. This enables appropriate actions to be undertaken for all reported disclosures to protect the IP and the interests of all relevant parties.

University of Sydney

- Appointed a Manager of National Security and Export Controls. The role supports work led from within the Deputy Vice-Chancellor (Research) portfolio on embedding defence trade controls, autonomous sanctions and foreign interference risk assessments, training and expert advisory into the University's higher risk research areas.
- Sydney applied for Defence Industry Security Program entry-level membership in October 2020. As part of those requirements, the University will be expanding new employee screening (to

Australian Standard 4811-2006) from all academics and those with financial delegations of >$100k, eventually to all new employees. Current employees who move part-time to full-time, or get promoted, will also get screened at these change points.

- Sydney is developing an integrated University International Collaboration intranet and education resource centre, as well as strengthening its external interest declaration and management processes and systems and processes for the 2020 exercise.
- Sydney consulted with staff on the university's proposed international collaboration principles. The principles will provide clarity and guidance for the university community in relation to any international collaboration that is undertaken through research, education, and other partnerships. Consulting with staff raised awareness as well as helped to ensure that the principles are beneficial to the university community. The university is also providing education and outreach about the Foreign Interference Transparency Scheme and the Guidelines to priority teams.

UNSW Sydney

- In July 2020, UNSW established the Division of Planning and Assurance (DPA). Led by the newly created role of Deputy Vice Chancellor, Planning and Assurance, the Division has been tasked with overseeing the assurance functions of UNSW, including legal, governance, records and archives, audit, risk and safety, to ensure that the changes are carried out in responsible and compliant ways.
- The Division will have oversight of all disclosures made by staff and is currently undertaking work to ensure that the policies relating to disclosures integrate with UNSW business practices and other policies requiring specific disclosures, including Foreign Influence, Commercial Activities and Third-Party Agreements.
- The Division is currently in the process of developing Foreign Influence Procedures and Guidelines to ensure compliance with UFIG. A new online process for staff to disclose foreign affiliations is being developed and information will be stored centrally on a secure register. A proposed Integrity Officer position within DPA will be responsible for managing this information and ensuring that disclosures are managed appropriately and escalated as required.
- Foreign influence matters at UNSW are covered by several existing policies including the Code of Conduct, Conflicts of Interest policy and the Research Code of Conduct.
- UNSW has developed and implemented robust risk management frameworks, policies, and practices, which cover the management of risk associated with international collaboration. The UNSW risk framework details the requirements for identifying, managing, and monitoring uncertainty. It clarifies how risk and opportunity are considered in strategic planning, review, approval, and execution of University, (and controlled entities [the University]) initiatives and the monitoring of operational performance. The Framework, adopting the ISO 31000:2018 principles, addresses how the University will embed the management of risk into their culture and practices and, by doing so, support the Executive and Council in making informed decisions and provide assurance that a robust risk management approach is adopted across the University. UNSW's Risk Management objectives include:
    - Risk tools that are customised and integrated into University processes whilst enabling consistency in the application of risk management principles. Most noticeably these include but are not limited to:

        - Strategic planning.
        - Anticipating and implementing strategic change initiatives, new commercial activities, ventures, and projects.
        - Assessing and introducing academic or administration changes to courses or processes, respectively.
        - Reviewing and approving research opportunities and grants.
        - Reviewing and assessing compliance controls and performance.
    - Building the required capability across the University to enable personnel to identify, assess and mitigate risks through providing tailored risk education and training.
    - Enhancing the risk culture through embedding a consistent application of the University's Risk Appetite into all strategic decision processes and facilitating salient risk discussions.
    - Ensuring a consistent structure for review and monitoring of treatment actions for those high and very high risks with a less than effective control environment and a potential to immediately impact (positively or negatively) the University's operations.
    - Ensuring the ongoing review and interrogation of the risk management performance against, available data/indicators, industry leading practices and feedback from stakeholders.
- The UNSW Research **Data Governance & Materials Handling Policy** covers principles related to maintaining the integrity, security, quality, and proper usage of research data and materials at UNSW. The purpose of the Policy is to:
    - Outline the requirements and roles and responsibilities associated with access, retrieval, storage, disposal, and backup of UNSW research data and materials
    - Provide best practice measures to enable compliance with the requirements
    - Ensure that UNSW complies with applicable laws, regulations, and operational standards.
- People working on UNSW Research Projects must refer to the Data Classification Standard and the Data Handling Guidelines for information on classification and security requirements. To comply with these requirements, they must:
    - Always use appropriate research data security measures to ensure the safety, quality and integrity of UNSW's research data and materials.
    - Store research data in an electronic format that is protected by appropriate electronic safeguards and/or physical access controls that restrict access only to authorised user(s), including research data in any UNSW or external data repository (databases etc.).
    - If research is undertaken in collaboration with other institutions, government agencies, or any third party, ensure that a written agreement is in place to cover research data and materials ownership, sharing, storage, accessibility, retention, and disposal.
- All researchers at UNSW are required to complete a research data management plan (RDMP).
- Research Data storage and access
    - Enterprise-level data systems (e.g., UNSW Data Archive, E-Lab Notebook) are fully compliant with data management requirements. However, some local specialist active

research data systems will require an uplift in capabilities to ensure all data is protected to the required level.

- Research Data management agreements
    - Many external collaborations are subject to formal written agreements (contract, MOU, other). However, research collaborations often begin less formally and rely on institutional research policies and codes of conduct to cover data management and access issues.
    - In order to address this, in 2021, the UNSW RDMP will be upgraded to
        - enable data management associated with external collaborations to be more clearly identified and documented
        - include new regulatory information as required by the Foreign Relations bill
        - include additional data management provisions required for defence research projects
        - where it is proposed to hold data offshore, provide a detailed justification
        - provide information regarding any data sharing agreements
- A program of work focused on the centralised management of third-party agreements is being developed in 2021 with a view to having a solution in place by 2022.
- Guidance is provided to researchers via our Research Data Management website: Research Data Management at UNSW | UNSW Research . Training and support is provided by the Research Technology team.

University of Queensland

- Program Due Diligence
    - To ensure appropriate disclosures of second academic appointments have been made in the Secondary Employment Register, an audit was undertaken to identify information that might indicate if a current UQ staff member holds, or has held, a foreign talent recruitment position. Where information suggested a foreign talent recruitment position may have been held, UQ has promptly investigated the specific nature of the appointment to ensure:
        - Staff are compliant with funding agency guidelines.
        - Staff are compliant with UQ's new policy framework on secondary employment requiring full disclosure and approval of the appointment.
        - The second institution involved is a suitable partner for the research activities being undertaken.
        - Appropriate arrangements were implemented to protect any intellectual property created and for alignment with the Guidelines.
- UQ has recently updated key policies to require the receipt of research funding, and the admission of Higher Degree by Research students, to be consistent with the Guidelines and applicable laws. This means that UQ may decline to admit a HDR student if, for example, the background of the student suggests an association with an institution with close ties to a foreign military, and the research is in a sensitive area.

- Export controls
    - UQ requires that researchers assess whether their work requires an export controls permit using The Defence and Strategic Goods Lists (DSGL) search tool on the Department of Defence's website.
    - UQ conducts information sessions in high-risk areas to ensure that researchers and students are educated about the nature of tangible and intangible exports of technology.
    - If permits are required, the researcher completes the online application and submits it to the UQ Director of Research Ethics and Integrity.
- Sensitive technologies
    - In addition to the DSGL, the Department of Defence has made a list of sensitive technologies available. While these goods are not included on the DSGL, UQ uses this list when assessing activities for foreign interference and associated national security risks and will contact the Defence Export Control Office (DECO) for an assessment prior to undertaking an activity based on a risk assessment of the partner involved.

Sanctions

- UQ has developed and implemented an assessment process for coursework students, staff appointments, casual academic appointments and international collaborations to ensure compliance with the sanctions regime. The process involves the completion of an assessment form and an assessment of the activity against the Consolidated List published by the Department of Foreign Affairs and Trade (DFAT).

Over the last two years, UQ has continued to strengthen its sanctions compliance system which includes:

- A review of how UQ meets its obligations under sanctions legislation across all areas of activity (Human resources, Teaching, and research) is being conducted by the International Safeguards Advisory Group.
- Development of a guide for international admissions staff as to the sensitivities of each sanctioned country in the legislation.
- Change to IT systems to flag students from sanctioned countries (e.g. a flag is raised if a student wishes to change course requiring another assessment, such as change from business to engineering).
- Change to placement offers to students from sanctioned countries (e.g. if the student wishes to change course, an assessment of the course will be made for sanctions compliance and it may not be available to the student depending on the nature of the course content).
- Change to placement offers to students from sanctioned countries who are undertaking coursework with a project component (e.g. the project chosen by the student will be assessed for sanctions compliance to ensure that the project complies with the sanctions laws and to ensure there is no access by the student to restricted equipment or technology).

University of Western Australia

- UWA has created a full-time International Compliance Officer position to manage defence research compliance and foreign interference work.

- Due diligence for international agreements
    - In response to the UFIT Guidelines, UWA has created a Foreign Interference Due Diligence Group (FIDGG) to review existing and planned international collaborations which meet certain thresholds – financial, research focus, partner entity, partner staff, number of students, among others.
    - This group, chaired by the University's Legal Counsel, also includes members of the Executive, research leaders with subject matter expertise, and researchers with language and other contextual skills which can help with assessments.
    - Where required, assistance is also sought from outside the University. Due diligence reviews conducted by FIDDG result in reports which highlight risks that may not have been apparent to the people proposing the collaborative activity, along with ways in which these risks can be mitigated. These reports have resulted in changes to some programs and in one program not proceeding.
- Defence Trade Controls
    - The University has web pages explaining the DCTA and our obligations under the Act. Grants are reviewed by the International Compliance Officer, who works with researchers to determine whether permits are required.
    - The International Compliance Officer also runs training for research groups who work on defence or dual-use technologies.
- Autonomous Sanctions
    - As autonomous sanctions apply to staff and to research students, there are separate processes for each, with the International Compliance Officer coordinating both and providing training for staff involved.
    - Research student applications are screened by the Graduate Research School.
    - HR sends requests for review of incoming staff from countries on the DFAT sanctions list.
- DISP registration
    - UWA has recently reviewed and strengthened its security for governance, personnel, physical and cyber security issues, through its registration with DISP.

Communication and Education

Australian National University

- The CSO has undertaken a range of briefings across campus on foreign interference.
- The University Research Committee has been involved in foreign interference policy discussions. A formal outreach program is being developed and will be launched in 2021.

University of Adelaide

- During 2020 and into 2021, the University response to the objectives of the Guidelines will focus on three main components:

- Review: Examining and changing as needed relevant policies, procedures and guidelines;
- Education: incorporating awareness of source and consequence of risk into relevant education and awareness resources or training; and
- Communication: promulgating consistent messaging across the University including to drive culture.

- The University of Adelaide's Legal and Risk department has updated its "integrity and accountability" website to better inform staff of integrity/accountability obligations that may be more difficult to recognise in the day-to-day pursuit of university objectives – highlighting foreign interference.

University of Melbourne

- A suite of Education and Training Programs are in place or in development to educate and increase awareness among staff and students of risks including: Research Integrity Online Training (RIOT); online modules such as 'Conflict of Interest – Research' and 'Key Policies and Information for Academics' and 'Managing Information – Cybersecurity' training for all staff.

Monash University

- Monash is working within a **communications framework** based on the pillars of awareness (equipping staff in various capacities with what they need know with relation to the UFIT guidelines, Foreign Relations Act, FITSA and so on), action (what they need to do – e.g. how to follow process for international agreements) and advice (where to seek help as needed). This work continues to evolve with the environment, for example, to incorporate the requirements foreseen under the *Australia's Foreign Relations (State and Territory Arrangements) Act*.
- Monash has embedded a comprehensive suite of **mandatory online training** for staff and students, including anti-fraud and corruption training, which is recommended for specific cohorts of staff (i.e., those with duties in areas in which foreign interference-related issues are more likely to be experienced).
- Updated Research Integrity training has been developed and made available within the Monash University suite of online training, which incorporates Conflict of Interest training and a training module on Export Controls.
- **Decision flow charts** have been developed to guide faculties in identifying projects that have potential foreign interference risks and the escalation pathway to Faculty Executives and the Transparency and Integrity Committee. Projects referred to the Transparency and Integrity Committee are required to fill in a preliminary foreign interference risk assessment form.
- **Regular briefings and guidance** have also been provided institutional and faculty leaders and key faculty and central staff, including Deans and Deputy / Associate Deans (International). For example, all faculty Deans have recently been given briefings on the content and anticipated requirements of the *Australia's Foreign Relations (State and Territory Arrangements) Act 2020*.

University of Sydney

- During 2019 and 2020 the University delivered numerous training sessions targeted at key teams about the requirement of the Foreign Influence Transparency Scheme and the Guidelines to counter foreign interference the Australian university sector.

- Detailed advisory information about the Defence Trade Controls Act and related laws is made available through the staff intranet with an on-line training module dedicated to this Act in the emerging national security environment close to completion.
- An integrated set of International Collaboration Principles has been developed to help guide staff and research students in their decision-making about international activities and is supported by a dedicated resources website available through the University's intranet.

UNSW Sydney

- The University is providing education and outreach about the Foreign Interference Transparency Scheme and the Guidelines to priority teams.
- Roll out of mandatory cybersecurity training for all staff and affiliates.

University of Queensland

- All staff are required to undertake training in Conflict of Interest Awareness (online) and Code of Conduct training as part of their induction.[1]

University of Western Australia

- UWA has conducted workshops on foreign interference risks to deliver an accurate understanding of the foreign interference risks that impact most on UWA and how UWA is or is not controlling these risks currently. This has resulted in the creation of a risk matrix, with risks and their controls assigned to named positions to manage.
- UWA has built on its existing program of training for defence researchers to include training on foreign interference risks for other researchers whose work potentially has a dual use, as well as administrative units which manage international issues such as donations, student recruitment, agreements, student exchange and similar.
- The University's actions and plans to manage foreign interference have been shared with Academic Board.
- The University has commenced development of an online staff training module on foreign interference risks

Knowledge Sharing

All Go8 universities are members of the Go8 Information Management Group, a key advisory group to the Go8 Board of Directors, which provides strategic advice and input to the Go8 Board on matters related to cybersecurity, foreign interference and influence issues on campus and in university operations.

They also access information through the UFIT process.

Additional examples from individual members include:

[1] https://staff.uq.edu.au/information-and-services/human-resources/induction-exit/starting/new-staff

Australian National University

- ANU has attended and shared information at sector wide forums on foreign interference methodology and risks.
- ANU enjoys a close relationship with several key government agencies on foreign interference matters and routinely shares intelligence

University of Adelaide

- On multiple occasions the University has consulted with the following Commonwealth departments and agencies to seek guidance on a particular activity:
    - Defence:
        - Defence Science Technology Group
        - Defence Headquarters
        - Defence Exports Office
        - Defence Export Controls Office
        - Defence Innovation Hub & Next Generation Technology Fund
    - ASIO
    - FITS Office

Monash University

- As part of the University's existing approach internationally, the University regularly seeks proactive guidance on relevant matters from government officials and agencies (both State and Federal) and particularly so when embarking on strategic international engagements of scale or where complexity warrants such interaction (research, educational or commercial). For example, when developing the Monash Technology Transformation Institute (MTTI) a R&D centre launched 29 May 2019 in the Pingshan District of Shenzhen, China, there was significant engagement with both the State and Federal government. Over a six-month period prior to its launch Monash engaged with 15 different agencies and Ministerial offices at Federal and State level to communicate the background and intent of the MTTI. These allowed these stakeholders to provide feedback and ask questions regarding the initiative.
- The Monash Research Office regularly engages with the Department of Defence on research projects relating to export controls, and also with the ARC and NHMRC on research integrity matters.

The University of Sydney

- Sydney presented on the 'Governance and Risk Framework' aspects of its response to the UFIT Guidelines at the inaugural Universities Australia's best practice workshop in October 2020. It has also contributed numerous examples of its activities to two Universities Australia reports on responses prepared for the UFIT.

- Sydney has shared much of its foreign influence and foreign interference training materials with other Australian universities and understands that some have adapted them for their own purposes.
- Numerous Sydney office holders and staff are members of NSW or national networks of university staff who hold similar positions. They routinely share insights and information through these networks formally and informally.
- Members of Sydney's leadership team have met with representatives from National Intelligence Community agencies to receive advice, share insights and information.
- Intelligence sharing is a particularly important part of Sydney's cybersecurity strategy, with the University engaging with the Australian Cyber Security Centre (ACSC) directly and through its membership of and participation in Joint Cyber Security Centre (JCSC) briefings and discussion forums. Within the sector, Sydney is an active member of the Australasian Higher Education Cybersecurity Service (AHECS), which serves as a forum for sharing insights on cyber security related technologies and services and a point of coordination for cyber security matters across the sector.

University of Western Australia

- UWA has worked closely with government agencies, the Go8, Universities Australia and other universities to share and learn best practice.
- The University has formed a working group with the other Western Australian universities to work cooperatively on these issues.
- UWA's cyber security team works with the Australian Cyber Security Centre and AusCert and engages fully in the University Foreign Interference Taskforce (UFIT) processes.

Cybersecurity

Australian National University

- In 2020, ANU commenced a five-year program to deliver a more cyber resilient campus.
- ANU consumes cyber threat intelligence from government and other commercial sources on a 15-minute update basis. Then University routinely shares threat intelligence with other universities and the Australian Cyber Security Centre (ACSC). ANU was also instrumental in helping to set up a national sector-wide intelligence forum.
- The University's cybersecurity program has a strong emphasis on building a positive secure culture. Under the program the University has released an initiative called Cyber Sense which had a soft launch this year and will have a formal launch in 2021.
- ANU utilizes the MITRE framework to develop threat models. The University will be linking this framework formally to business risks in the University's risk register in 2021. That said the University's capability model already links dimensions of business risk to guide cyber related investment.

University of Adelaide

- The University "Secure IT" website, hosted by Information Technology and Digital Services, provides a range of information and advice on secure computing practices to be safe online. This includes advice on being safe while travelling, recognizing phishing scams and malicious emails, and selecting a secure password[2].

- All staff are required to complete an online cybersecurity tutorial[3].

University of Melbourne

- The **Chief Technology Officer** is overseeing a 5-year program (currently in year 2) to uplift cybersecurity capability across the institution to prevent, detect, and respond to cyberthreats. This program is working with stakeholders across the University to make the institution less vulnerable to cyber threats while balancing its need for openness, autonomy, and collaboration. It will include new and upgraded technologies and education materials, as well as a refresh of policies, processes, and guidelines.
- As part of this program of work, **mandatory Cybersecurity e-Learning module** training for all continuing and fixed-term academic and professional staff was developed and rolled out across the institution in late 2019. As of May 2020, 86% of University staff have completed the Cybersecurity training module. This includes 91% of Professional and 81% of Academic staff.

Monash University

- Monash has adopted a globally recognised industry cyber security framework, the **National Institute of Standards and Technology Cybersecurity Framework** (NIST CSF). An organisation-wide assessment using the NIST CSF has been undertaken and used to measure the University's cybersecurity maturity, identify areas for improvements and compare the University to peer organisations. The data from this assessment is a key input into the University's Cyber Security Strategic Plan. The University appointed the Chief Information Security Officer in November 2019. A new Cyber Awareness role has been established and filled in late May 2020. This role leads the existing Cyber Awareness Program for staff and students and will form part of the three year Cyber Security Strategic Plan.

- Monash currently holds the **ISO 27001** (information security standard) certification for specific research platforms and the supporting infrastructure. This is very rare in the higher education sector and Monash has maintained this certification for seven consecutive years.

- Monash has received the highest rating of 'Embedded' for a **Defence Industry Security Program (DISP)** membership. Membership of DISP requires a high degree of certified cyber security rigour. Monash's rating means that all Defence Security Principles Framework (DSPF) requirements have been met or exceeded and that Monash's IT and cyber security standards are high enough within the Secure Data Enclaves (SDE) platform to work on Defence research and allows Monash to handle Protected Defence information.

[2] https://www.adelaide.edu.au/technology/secure-it
[3] https://www.adelaide.edu.au/technology/secure-it/cybersecurity-training

- Monash has developed a strategic, holistic and long-term sustainable approach to cybersecurity, culminating in the development of a cybersecurity strategic plan for the University. The three-year Cyber Security Strategic Plan (2021-23) has been approved and will be delivered in Q1 2021. The objective of the Strategic Plan is to ensure that the University achieves a balance between the drive for digital innovation, agility, and openness; and the appropriate and proportionate protection of University systems, information, and reputation.

University of Sydney

- Sydney is delivering an integrated suite of cybersecurity projects under four streams (phishing, risk, governance and advanced threat protection) to address priority threat scenarios identified through an independent review conducted in 2019. This includes the roll-out of annual mandatory cybersecurity training for all staff and affiliates.

- Cyber security is one of Sydney's highest priorities, and crucial to its core mission – to excel as a world-renowned research and teaching institution. Its cyber security policy framework encompasses technical, procedural and personnel controls across all National Institute of Standards and Technology's (NIST) Cyber Security Framework control domains. Its defence-in-depth approach recognises that preventive measures cannot provide absolute protection from highly skilled, resourced and motivated threat actors. Consequently, Sydney's internal cyber security team works closely with managed security service providers to deliver continuous monitoring, incident detection and response capabilities to the University. The implementation, maturing and improvement of these advanced security operations capabilities is key to improving our ability to rapidly identify and respond to threat actors targeting our staff, students, researchers and information.

- Sydney's management of cyber security risk is underpinned by comprehensive threat modelling using Factor Analysis of Information Risk (FAIR), an internationally recognised model for understanding, analysing and quantifying cyber security risk in financial terms. The modelling was developed in collaboration with PwC and is regularly updated to reflect changes to cyber security threats, the legal and regulatory environment, and the results of control assurance testing. The results of the threat modelling are used to report on risk exposure to the University Executive and Senate and to inform prioritisation and investment in risk treatment initiatives.

- Building awareness of cyber security risk at senior levels across Sydney University has been achieved through the inclusion of cyber security risk on the enterprise risk register, and the corresponding consideration of risk acceptance and mitigation plans by relevant University Executive and Senate committees. Regular in-person briefings have been provided to faculty management and researchers, helping to develop a stronger cyber security culture.

- Sydney achieved a significant milestone in 2019 with the implementation of mandatory annual cyber security training course for our staff. This broad-based training has been supplemented with regular internal communications and more targeted threat-specific training in areas such as email phishing.

UNSW Sydney

- Cybersecurity protocols have been developed for UNSW users in China, aimed at ensuring the security of the University's information assets and prevent information from being maliciously vandalised, stolen or inadvertently damaged. The protocols target individuals that have been authorised to use or access UNSW Information systems in the UNSW China offices and individuals from the University's Australian based campuses that are travelling to work in China and have been authorised to use or access UNSW information.

- A strategic security awareness training program is currently being developed and will have modules aimed at travelling employees who take corporate devices and data on the road. This includes recommendations such as taking disposable or clean devices when travelling, disabling Bluetooth, built-in cameras and microphones and never leaving devices unattended.

- Security and infrastructure monitoring capabilities are being investigated to protect UNSW data, intellectual property and access to UNSW systems and environment for a specific list of overseas users, particularly located in China.

- Due to security concerns, Huawei equipment and solutions for storage platforms and its usage for Research Domain and UNSW will not proceed.

University of Queensland

- UQ is strongly committed to effectively managing and reducing cybersecurity risks.

- In 2017, UQ published a **three-year Cyber Security Strategy**. The Cyber Security Strategy recognises the risk and increasing prevalence of cyber-attacks. It identifies foreign interference as one of the key factors influencing strategic direction and commits UQ to compliance with the Guidelines. The Cyber Security Strategy is currently being updated.

- As part of the Cyber Security Strategy, UQ maintains a detailed cybersecurity risk register to track and improve its risk profile. Progress is tracked via quarterly reports to executive management and risk committees. Work is planned to generate additional operational security metrics to assess the effectiveness of cybersecurity controls. UQ also maintains a critical information asset register, which informs protection requirements. Both registers are constantly being reviewed.

- UQ employs a range of technical and administrative security controls to protect information, detect threats, respond to, and recover from incidents. It performs security testing against systems, processes, and people to determine its vulnerability to cyber threats. The results of those tests are used to measure and improve protections.

- The investment in Australian Academic and Research Network-managed Security Operations Centre is key to UQ's strategy to improve its detection capability. It provides a scalable approach to augment UQ's in-house security operations capability. It is anticipated that as the Security Operations Centre starts to leverage intelligence from multiple universities as well as university internet traffic, it will be able to deliver a highly effective detect and response capability across the sector.

- UQ participates in a number of surveys to benchmark itself against other universities and organisations, and is consistently in the top quartile of cyber secure universities, including the Go8.

- UQ receives intelligence on cyber security threats from many different channels, including the Australian Cyber Emergency Response Centre, the Australian Cyber Security Centre, the Australian Security Intelligence Organisation and the Research and Education Networks Information Sharing and Analysis Centre.

University of Western Australia

- Cyber security at UWA is driven by University IT's Cyber Security & Technology Risk function, mandated to protect digital IT assets to an extent determined by the University's risk appetite. Cyber security works in close collaboration with the following organisational functions to enable protection of the University's IT assets:
    - Information Governance provides the basis for managing information throughout its lifecycle – such as information classification and handling, records management and privacy requirements;
    - Human Resources drives personnel security – such as employee screening, training and disciplinary processes;
    - Campus Management ensures the physical security of IT assets – such as building security and physical access management.

- The University's Cyber Security Policy outlines its commitment to preserving IT assets and mandates the implementation and continual improvement of a formal Cyber Security Management Framework (CSMF) based on the ISO27001 Standard to establish risk-based security capabilities, practices and responsibilities. It looks to implement a risk-based improvement in capability across:
    - Security governance,
    - Awareness and culture,
    - Cyber hygiene, and
    - Identity and access management.
- The development of a suite of core security metrics and automated reporting capability is currently in progress.
- UWA Cyber Security unit provides:[4]
    - Cyber Security awareness and training;
    - Cyber Security consultation services; and
    - Cyber Security incident management and response.

[4] https://cybersecurity.it.uwa.edu.au/

Case studies / examples of proposals that Go8 institutions have refused or altered on the basis of foreign interference concerns

These examples have been de-identified.

- One member university has established a research and research training agreement with a faculty at an overseas university. Open-source intelligence indicates that this overseas university faculty conducts military-linked research in some specific disciplines. A different section of the overseas university works with its home government's military on hacking and cybersecurity. Through enhanced due diligence processes, the university has highlighted this risk to their staff (researchers and administrators), resulting in:
    - research in areas linked to the overseas university's military research being excluded from the research collaboration;
    - careful consideration of all topics for potential 'dual uses';
    - enhanced security measures for staff for the overseas university who access their IT systems; and
    - enhanced IT security for their staff visiting the overseas university.
- Another member university:
    - Declines to engage with prospective Higher Degree Research Students, if for example, the background of the student suggests an association with an institution with close ties to the military, and the proposed research is in a sensitive area;
    - Declines to support second appointments if the research proposed is in a sensitive area (among other reasons);
    - Makes appropriate FTE adjustments and requires restrictive intellectual property agreements to be put in place as the basis for giving approval to some joint appointments.
- Other examples include:
    - **International Collaborations** – the membership of research teams collectively submitting bids for Federal funding have been rearranged by dropping collaborators based on their institutional affiliations.
    - **Defence Export Controls (DEC) Review** – despite research not involving controlled sensitive technology, DEC advice has been sought and provided on research involving international research collaborators who may be involved in other activities invoicing sensitive technologies. DEC's advice enhanced contract provisions and business processes to protect both Australian intellectual property and the member university's reputation.
    - **Computer Vision** – a researcher was approached by an international telecommunications company regarding research on visual speech recognition. The project was referred for assessment to relevant leadership and research governance functions in the university. Concerns were raised regarding both the company and focus of the research and a decision was made not to proceed.

Examples of penalties applied when university policies are breached

Breaches of institutional policies at Go8 universities can lead to significant penalties. In the interests of brevity, indicative examples are provided from three member institutions:

UNSW Sydney: Policies and Codes in place covering Foreign Interference

Foreign Influence matters at UNSW are covered by a number of existing policies including the Code of Conduct, Conflict of Interest policy and the Research Code of Conduct.

If a staff member breaches the Code of Conduct, the University may take disciplinary action. In serious cases, this may include termination of employment. The process for dealing with alleged breaches of this Code by staff will be in accordance with the applicable enterprise agreement, industrial instrument or contract.

Failure to comply with the Conflict of Interest Policy may lead to:

- misconduct or other disciplinary procedures which may include termination of employment;
- referral to and action being taken by external agencies such as the Audit Office of NSW, ICAC and the NSW Ombudsman, and/or notifications to ethics committees, journals/publishers and funding agencies such as the ARC/NHMRC; and/or
- legal action by third parties against UNSW and/or the individuals concerned.

Any suspected or potential breach of the Research Code will be managed in accordance with the UNSW Research Misconduct Procedure.

University of Queensland

If a risk is identified, UQ will take appropriate remedial action including investigating the matter and referring to the grant bodies and regulatory authorities in accordance with applicable laws, funding guidelines and its policies and procedures including the Managing Complaints about the Conduct of Research Procedure, staff misconduct and serious misconduct processes in the UQ Enterprise Agreement 2018 – 2021, Research Misconduct – Higher Degree by Research Students Procedure and Student Integrity and Misconduct Policy.

Monash University

In cases of conflict of interest where the conduct can be classified as misconduct or serious misconduct, the matter will be referred for consideration under the University's staff disciplinary procedures, which can result in escalating disciplinary actions, including formal censure; withholding of an increment; suspension with or without pay; and/or termination of employment.

The University has a suite of research specific policy and procedures which includes topics such as Sanctions, Defence Trade Controls, and research funding. Policy breaches are considered breaches of the Code for the Responsible Conduct of Research and managed accordingly.