# GUIDELINES ON SECURITY IN THE CRC PROGRAM

**Overview**

This document has been prepared to provide some direction to Cooperative Research Centres (CRCs) in relation to security matters in the Cooperative Research Centre Program (CRC Program). It is ultimately the responsibility of individual CRCs to make their own independent inquiries and obtain their own independent professional advice prior to relying on, or making any decisions in relation to, the information provided in this document in developing their own security and risk plans.

The most recent Round 21 & Round 22 grant agreements state:

*The Grantee must ensure that at all times the Grantee and partners have appropriate measures in place to protect any Activity Material related to national security.*

*The Grantee must ensure it has a plan to manage and monitor the project including risk management of but not limited to security (in particular any associated national security issues), and involvement of international partners and intellectual property protection.*

With this in mind, the following information has been prepared to guide CRCs' understanding in this new requirement and to inform quarterly reporting statements.

National security protects the national interest and includes protective security and other means available to the national security community. Intellectual property is generally not addressed here, unless it includes matters pertinent to national security (where it should be protected by more than a patent, copyright or some other type of property right). The approaches to protective security are based on the:

- Australian Government's Protective Security Policy Framework;
- Information Security Manual (ISM); and
- associated strategies to mitigate cyber security incidents (Essential Eight Maturity Model).

National security is about protecting our broader national interests. National interests are not only intrinsically valuable, but include things which are valuable to us, attractive to others and sometimes dangerous if mishandled. National security is important because it helps keep these things safe and secure. Things which may require protection include people, physical assets and information (hardware, software and data). The latter covers cyber security and data risk, potentially including **sensitive** data-sets of national importance, such as mapping of resources like land, sea, energy networks and infrastructure.

In developing their own Protective Security Framework, CRCs should be consistent at least in principle with the Australian Protective Security Policy Framework. Security measures should be proportionate to the assessed risk and minimise any impact on innovation, collaboration and cooperation

**Mapping the national interest/security environment**

The CRC Program is the Australian Government's flagship for business-research collaboration and benefits Australia's national interest in many areas (e.g., environmental, economic, scientific and technological). The CRC Program encourages participation from a diverse range of organisations to maximise the potential for innovative outcomes. Through the CRC Program, new technologies, products and services are being developed, new and global markets are being accessed, and by investing in R&D, businesses are increasing their income, competitiveness and productivity. CRCs are building capability and capacity for industry through targeted education and training activities, while sustainability and the environment also benefit.

CRCs provide industry-focused education and training opportunities. All CRCs are required to have an education and training program, including a requirement for a PhD program. CRCs develop undergraduate courses aimed at filling an identified gap for the targeted industry. The education and

training program complements the research program and increases engagement, technology development, R&D capacity within industry entities and employee skills.

International engagement and collaboration has been a core element of the CRC program. CRCs are encouraged to collaborate and co-invest with international organisations and businesses to assist industry partners to engage with global supply chains and access new markets. They engage in a diverse range of collaborative activities with foreign and multinational businesses, including:

- joint research projects and commercialisation activities as partners;
- providing access to research facilities and infrastructure (some located overseas);
- participating on international committees and advisory boards; and
- conducting joint workshops, study tours, student placements and exchanges.

Some CRCs are engaged in areas of research relevant to national interest, including some at the boundaries of current human understanding (e.g., quantum computing, artificial intelligence and hypersonics). Additionally, some CRC personnel may have a rare and valuable understanding in areas which would be difficult to replace. There are also risks associated with the loss of assets, which could cause financial, reputational and other damage. These rare and valuable people, information and other assets can be important to our national interest. If so, investment in protecting these is warranted and CRC risk management planning should identify them as something to be kept safe and secure, evaluate the risk and treat it appropriately (e.g., have proportionate controls in place to address any existing or emerging areas of concern).

Contributions made by partners to a CRC established as a company limited by guarantee for the purposes of undertaking collaborative research do not appear to be subject to the *Foreign Acquisitions and Takeovers Act 1975* and therefore, not requiring Foreign Investment Review Board (FIRB) approval. However, this guidance is generic and does not consider any particular structures and/or governance arrangements of the various CRCs. If a particular CRC, or participant in a CRC, is concerned a contribution to a CRC by a foreign person may require FIRB approval then that CRC, or participant, should obtain their own independent legal advice.

**National Interest and (National) Security: keep these in mind, at a proportionate level**

Security plans should include governance arrangements, and information (including cyber), personnel and physical security. The security plan reflects a CRC's protective security requirements and mitigation strategies appropriate to the levels of threat, risks to its assets and risk tolerances. CRCs are encouraged to use approaches which manage risks and reflect their operational environment.

The security effort should generally be proportionate to the interests being protected. CRCs would be expected to report to the department any significant change in their security circumstances (e.g., changes to key personnel, information security, physical security, financial arrangements, etc.).

**National security risk assessment**

Risk is assessed through the equation: **Risk = Threat × Vulnerability × Consequence**.

**Threat** assessments examine the intent and capability of malicious actors to conduct sabotage, espionage and/or coercion against the CRC, or its constituent parts. Intent is the desire and likelihood of the actor to proceed with their plans, while capability is the actor's skills and resources which enable it to carry out its plans.

**Vulnerability** is an assessment of the CRC attributes to determine points of weakness which the threat could exploit and the level of protection from the threat.

**Consequence** is the outcome or impact on national security if an event linked to the CRC was to occur. Based on a CRC's overall risk rating and whether the level of risk is tolerable. The risk treatments should always be proportionate and effective, with consideration given to minimising any additional burden to mitigate the national security risks identified. Similar considerations would also apply to minimising any market distortion and to ensure unnecessary burdens are not imposed.