# GUIDELINES ON SECURITY IN THE CRC PROGRAM

March 2021

## Overview

The CRC Program is the Australian Government's flagship program for business-research collaboration. The innovations and research partnerships CRC Program participants (CRCs and CRC Projects) develop have enormous potential to boost the growth of industries, create jobs and improve the lives of Australians. Because their work is so important, the outputs of CRC and CRC Project (CRC-P) collaborations can be an attractive target for foreign interference and intelligence gathering.

The Department of Industry, Science, Energy and Resources has developed these guidelines to help CRC Program participants consider national security risks. These guidelines represent a starting point, but each organisation will face unique circumstances. Each CRC Program participant should make their own enquiries when formulating security plans.

Considering national security protects Australia's broader national interests from those intending harm. National interests can include people, physical assets and information. Cyber security risks are particularly important and CRC Program participants should ensure they appropriately protect sensitive datasets, which can include maps of strategic resources like land, sea, energy networks and infrastructure assets.

## Developing a security plan

CRC Program participants should consider their strategic goals and objectives when developing security plans, and take a risk management approach. Plans should be consistent with the Australian Government's Protective Security Policy Framework and address risks relating to governance, information (including relevant cyber security risks), personnel and physical security. CRC Program participants should share their security plans across the collaboration, particularly with partners and staff with responsibilities identified in the plan. This will help build a positive security culture based on a common understanding of risks.

A security plan should be a 'living' document, reviewed regularly to ensure it remains fit-for-purpose. CRC Program participants should review security plans at least every two years or when there are significant shifts in risk or operating environment. Security risk mitigation strategies should be proportionate to the assessed risk, and implemented to minimise the impact on innovation, collaboration and cooperation. Ultimately, security risk management planning should identify what needs to be kept safe and secure, evaluate the risk, and determine appropriate controls to mitigate against the identified risks.

## Measuring risk

Risk can be considered as a combination of threat, vulnerability and consequence.

- Threat assessments consider the intent and capability of malicious actors to conduct sabotage, espionage or coercion against a CRC Program participant. Intent covers the desire and likelihood of the actor to proceed with their plans, while capability covers the skills and resources with which the actor can carry out their plans.
- Vulnerability is an assessment of a CRC Program participant's 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 the identified risk occurs. Consequence assessments should consider the impacts to Australia's national security, not only the consequences to a CRC Program participant. The assessment should also take into account the potential physical, social, economic and governmental impact on Australia.

Common risk indicators which CRC Program Participants should be aware of when developing their security plans include:

- New relationships which develop quickly into significant opportunities.
- People asking questions about other lines of activity unrelated to the primary project or research.
- People exhibiting an unusual interest in specific technical know-how, the application of technologies, or cultivating relationships with staff.
- Attempts to access sensitive or secure areas, offers of free ICT equipment to connect to the CRC Program participant's network, or offers to host the network or data on foreign-owned systems. (Check the Australian Government's Information Security Manual (ISM) for further advice)

## Developing a security plan

When developing a security plan, it may be helpful to consider the questions below.

*For your CRC Program partners, key personnel and researchers:*

- Have you undertaken appropriate due diligence? The Australian Security Intelligence Agency (ASIO) Due Diligence Integrity Tool was developed as guidance for Australian institutions which are considering engaging with foreign entities. The tool provides a framework to consider some of the security risks associated with foreign collaboration. Please contact the ASIO Outreach Team at outreach@asio.gov.au for a copy of the ASIO Due Diligence Integrity Tool.
- Is their interest in the CRC Program aligned to their stated business or research activities?
- Can others in the industry sector provide insight into their background or credentials?
- Do you know who they work for or represent?
- Are they receiving any foreign financial support for research or other activities?
- Are they currently, or have they previously been, associated or affiliated with a foreign sponsored talent-recruitment program, foreign government, foreign political party, foreign state-owned enterprise, foreign military or foreign policy organisation?
- Do they work to Australian and global moral and legal standards? Are they subject to any Australian or international sanctions?

*For your research, technology and knowledge:*

- What are the potential benefits of your research, technology or knowledge?
- How could others use or apply your research, technology or knowledge?
- Does your research, technology or knowledge:
    - fall under export control regimes?
    - have dual-use potential?

*For the appropriateness of identified risk mitigation controls:*

- Will the controls and respective implementation strategies effectively minimise the risks? How could you improve the controls?
- Are the controls comparatively efficient and cost-effective?
- Are the controls proportionate with the identified risks?
- Do the controls comply with policy requirements, legal obligations and internal operational procedures?

- How frequently will you test or review the protective security arrangements and risk management processes?

## Getting further assistance

There are a range of resources available to help better understand national security issues which may apply to businesses and organisations. You can consult the Australian Government's Protective Security Policy Framework and Information Security Manual. You can also:

- Subscribe to the ASIO Outreach Service to access protective security advice and assessments.
- Contact the Australian Cyber Security Centre for more information and cyber security advice by calling 1300 CYBER1 (1300 292 371).
- Visit the Department of Home Affairs' Countering foreign interference website.
- To assist with managing security risks, you also are strongly encouraged to review the department's *Guide to undertaking international collaboration*, as well as the *Guidelines to counter foreign interference in the Australian university sector* developed by the University Foreign Interference Taskforce (UFIT). Although focused on the university sector, many objectives and best practice considerations in the UFIT guidelines are applicable to other research institutions and businesses.