Australian Government
Department of Defence

SECURITY REQUIREMENTS
FOR DEFENCE COLLABORATIVE RESEARCH

Defence has a responsibility to protect information and intellectual property generated or exchanged through research collaborations. Defence personnel initiating collaborative research are required to familiarise themselves with their responsibilities under the Defence Research Collaboration Security Framework.

Defence employees are required to:

- Determine the sensitivity of and protection required for collaborative research on a case-by-case basis:
  - Apply the Defence Research Collaboration Security Framework to support the security assessment
  - Conduct sensitivity assessments for all collaborative research proposals
  - Conduct security risk assessments, where required
  - Ensure that appropriate security arrangements are included in the research collaboration contract
- Provide clear advice to collaborators on the security requirements for collaborative research
- Consider and manage residual security risks

Research collaborators may be required to:

- Agree to implement the protection requirements specified by Defence for collaborative research
- Become a member of the Defence Industry Security Program (DISP)
  - Obtain entry-level DISP membership, initially
  - Consider DISP membership at higher security classifications
- Consider obtaining higher level security clearances for key staff and researchers
- Collaborate with other universities, industry and state-based networks to coordinate and leverage security investments

Further information:

Allan Halsey
Director, Defence Research Collaboration Security
allan.halsey@dst.defence.gov.au
08 7389 5020

DSC2382

Australian Government
Department of Defence

Defence Research Collaboration Security Framework

FREQUENTLY ASKED QUESTIONS

Why do we need to change how we protect Defence collaborative research?

- Defence research collaboration is evolving and is moving into more sensitive and nationally classified areas. This research has a significant positive impact on defence and national security capabilities and operations by providing a "technology edge", but comparative advantages will only be maintained where the research and its application is appropriately protected from access by potential adversaries and competitors.
- The Defence Research Collaboration Security Framework will provide guidance and processes to assess the type, category, sensitivity or security classification and risks to information likely to be generated or exchanged through research collaboration.
- The change we are making will ensure that our security protections and those applied by our collaborators are contemporary, aligned with the Defence Security Policy Framework (DSPF), the Defence Industry Security Program (DISP) and are appropriate to the research being conducted. These arrangements are necessary to ensure that :
    - Security risks are understood and are mitigated to an appropriate level.
    - Defence and national security technology edge, capability and investment are not compromised.

Is it true that all DST research conducted with collaborators needs to be protected?

- No, that is not true.
- Some of DST's research collaborations will remain "Unclassified and suitable for public release". This type of research does not require additional protection.
- What is true is that all DST research that is being proposed to be conducted with an external collaborator needs to go through the Defence Research Collaboration Security Framework processes to determine the security protections that will be required.

Is it true that all Defence Intellectual Property needs to be protected?

- DST policy, as outlined in DST Group Instruction 003/2020 stipulates that where Intellectual Property (IP) is generated or exchanged as a part of a research collaboration, it will be assessed as sensitive and the minimum security protection to be applied is DISP entry level.
- If the IP is classified Protected or above, the IP must be protected by our collaborators by achieving and applying the required level of DISP membership.

When will an "assessment" of the research collaboration activity be required?

- All DST collaborative research agreements must include an assessment, which identifies the type, category, sensitivity or security classification of the research and, where necessary, the security risks to information likely to be generated or exchanged through the collaboration.
- This assessment is known as a "Sensitivity Assessment". One of the outcomes of the SA will be to determine the security requirements to be applied by the research collaborator.

Will all research collaborators need to get a security clearance?

- Research collaborators will need to obtain a security clearance if it is specified as a requirement to participate in the research. These requirements will be developed as a part of the sensitivity assessment.
- Where DISP Entry level protection is required a minimum of a BASELINE security clearance will be required to participate in the research.
- Higher levels of protection will often require participants to have higher security clearance levels and achieve higher levels of DISP membership.

DSC2382