



Defence Intelligence Organisation Mandate

The DIO Mandate describes DIO's role, operating context, functions, organisational character, analytical independence, tradecraft, analytical standards, and governance and assurance arrangements.

Role

DIO is Defence's all-source intelligence assessment agency. DIO's role is to provide well-judged, clear and timely insights into defence and security-related matters that may affect Australia's national interests. DIO's assessments must enable ministers, policy advisers, capability managers and military commanders to make informed decisions. DIO works primarily at the strategic level; it must also work to support the operational and tactical domains.

Operating context

DIO is part of the broader Defence Intelligence Group. DIO's unique value-add in Australia's National Intelligence Community (NIC) is its expertise as a world-class defence intelligence assessment agency. DIO collaborates closely with the broader Defence intelligence community, and with NIC and international partners in support of Government and Defence priorities.

The strategic environment

Australia is at the centre of a dynamic strategic environment. Our strategic circumstances are not benign. The prospect of a high-intensity conflict in the Indo-Pacific region is less remote than in the past. Coercive statecraft, military modernisation, state insecurity and the use of cyber-enabled disruptive technologies challenge our national interests.

Functions

DIO provides insights into the current and planned capabilities and intentions of state and non-state actors who may affect Australia's national interests. DIO's assessments provide strategic warning, they inform the development of defence policy, the planning and conduct of defence operations and activities and guide capability development through their insights into:

- foreign government decision-making, as well as strategies and plans for the use of national security forces
- foreign military and security forces' doctrine and operating concepts
- the threats posed by potential adversary weapons systems and capabilities
- the operating environments in which Australian defence capabilities are, or may need to be, deployed.

DIO works in collaboration with Defence and international partners to generate foundational intelligence mission data that underpins the lethality and survivability of the ADF's advanced weapons systems.

In support of whole-of-government decision-making, DIO contributes assessments and analysis on:

- international counter-terrorism capabilities and efforts to counter terrorism
- threats from weapons of mass destruction and their proliferation
- sensitive defence and dual-use equipment and technology of proliferation concern
- warning and monitoring of diseases of national and military significance, including pandemics
- foreign cyber threats to the Australian Government and its interests.

DIO's expertise may also contribute to other government priorities such as countering coercive statecraft; and the national security implications of technology development to aviation security, risks to defence industry and supply chain vulnerabilities.

Analytical independence and standards

DIO is not subject to direction in regards to the judgements in its intelligence assessments. Analytical independence is a key tenet of DIO's assessment function. DIO assessments must be independent, clear and concise, timely, insightful, based on all available sources, accountable and rigorous.

International relationships

DIO collaborates closely with a wide range of international partners and organisations. This includes our traditional Five-Eyes partners. DIO also engages with other like-minded countries and close regional partners on issues of mutual strategic interest. DIO must seek approval from the Minister for Defence to formalise such relationships.

Governance and assurance

DIO adheres to the highest standards of individual and organisational culture. DIO conducts its work consistent with Australian Public Service and Defence values. DIO adheres to:

- privacy rules
- protection of classified materials
- protocols for the use of open source information.