Job description

Haere mai

This job description is your go-to place for all the ins and outs of this role at Internal Affairs

Principal Advisor (Countering Violent Extremism), Digital Safety

Regulatory Services, Toi Hiranga|Policy, Regulation and Communities

Regulatory Services has oversight of three regulatory systems: Anti-money laundering and countering the financing of terrorism, Gambling, and Digital Safety (anti-spam and censorship). We are a responsive risk-based regulator focused on reducing harm and ensuring that iwi, hapū and communities across New Zealand are safe, resilient, and thriving.

Our vision for the digital safety system is to make the digital world a safer place for everyone. You will support the Director by providing thought leadership and utilising your established national and international networks to build the CVE capability of the Digital Safety Group, the wider digital safety system, and promote best practice nationally and internationally.

- **Reporting to**: Director Digital Safety
- **Location:** Wellington
- **Salary range:** Regulatory J (1-year fixed term)

What we do matters – our purpose

Our purpose is to serve and connect people, communities and government to build a safe, prosperous and respected nation.

In other words, it's all about helping to make New Zealand better for New Zealanders.

How we do things around here – our principles

We make it easy, we make it work

- Customer centred
- Make things even better

We're stronger together

- Work as a team
- Value each other

We take pride in what we do

- Make a positive difference
- Strive for excellence

Te Tari Taiwhenua
Internal Affairs

Working effectively with Māori

Te Aka Taiwhenua – our Māori Strategic Framework – enables us to work effectively with Māori. Te Aka Taiwhenua is underpinned by our mātāpono – Kotahitanga, Manaakitanga, Whānaungatanga, He Tāngata.

As DIA is an agent of the Crown, Te Tiriti o Waitangi/The Treaty of Waitangi is important to everything we say or do. We recognise it as an enduring document central to New Zealand's past, present and future. Building and maintaining meaningful relationships is important to work effectively with Māori, stakeholders and other agencies. We accept our privileged role and responsibility of holding and protecting the Treaty of Waitangi / Te Tiriti o Waitangi.

What you will do to contribute	As a result, we will see
A trusted advisor with specialist knowledge and experience • Work effectively with diversity, and include diverse people, thinking and perspectives into the regulatory activities needed to keep them safe • Provide intellectual leadership and deep specialist knowledge to build capability (people, processes, and systems) to enable the Countering Violent Extremism (CVE) functions within the Group • Ensure DIA follows, where possible international best practice in a way that meets our roles and responsibilities as a risk-based responsive regulator • Knowledge sharing across the Group to support the ongoing capability of the CVE function including understanding current and new trends in CVE, new technologies and techniques across the global CVE eco-system • Apply existing knowledge of latest evidence-based practices, innovative approaches and concepts that involve disruptive digital technologies to improve the effectiveness of our regulatory approach and practices	• The Group has agile processes and systems that are practicably reflect best practice and evidence-based research • The Intelligence and Insights Manager, and the Manager Digital Violent Extremism report your support to build their teams • The Group's CVE capabilities fit with security and regulatory practices • The Group's staff report positive experiences with coaching, mentoring and feedback • The CVE and CT regulatory work of the Group is of high quality, has integrity, and supports the effectiveness of results on community outcomes

What you will do to contribute	As a result, we will see
System leadership and collaboration • Support the Director DS and wider CVE system by providing up to date advice and information that is tailored appropriately communicated for the audience and supports our regulatory role in CVE digital safety eco-system • Use existing established CVE and CT national and international relationships and networks and develop processes and systems for Digital Safety to learn and manage those relationships and networks successfully • Actively support the Director Digital Safety by managing critical CVE stakeholder relationships nationally and internationally • Work within the Group and with our national and international partners to support and initiate the development of innovative CVE operational strategies and/or products to achieve the digital safety system outcomes • Collaborate with partner agencies to establish opportunities and processes for digital safety system leaders to gather and share information and establish ways of working together on joint responses to CVE events and/or investigations	• Strong support for our CVE and CT regulatory work from partners and national and international networks and stakeholders • Partner agencies working together effectively to advance CVE outcomes • Relationships and networks are used effectively to achieve community outcomes • Evidence of effective collaboration with partner agencies both nationally and internationally reflecting a joined-up relationship • The Group has the capability to develop, manage and monitor its own networks, partners and stakeholders effectively • Your advice helps support the success of the Christchurch Call-international and nationally
Responsive, risk-based regulation and stewardship • Inform and lead the establishment of innovative operational strategies that reduce the risk of harm from digital violent extremism – including using current research and techniques for disrupting violent extremism or for countering terrorism • Develop regulatory responsive risk-based approaches that are appropriate in the circumstances and support the making of relevant guidance to support the key operations of the group • Support the Director Digital Safety by assessing, identifying and mitigating risk attached to the CVE and CT systems, ensuring that key mitigations are fit for purpose	• Innovative and current CVE operational processes and systems that reflect best practice are developed and implemented • The Director and Managers receive timely alerts to any real or potential risks relating to the systems and services run or delivered by the Group • Any mandate, policy, legal, ethical or logistical issues arising from investigations or operations are fully considered and escalated where appropriate

What you will do to contribute	As a result, we will see
Health and safety (for self) • Participate in the mandated psychological supervision programme. Co-operate in implementing the rehabilitation plan • Work safely and take responsibility for keeping self and colleagues free from harm • Monitor, encourage and engage colleagues working with objectionable material to have regular debriefing or counselling to ensure their ongoing well being • Report all incidents and hazards promptly • Know what to do in the event of an emergency • Cooperate in implementing return to work plans	• A safe and healthy workplace for all people using our sites as a place of work. • Health and safety guidelines are followed • You can deal successfully with highly stressful environments, including dealing with objectionable material of violent extremism (including possible loss of life situations)

Who you will work with to get the job done		Advise	Collaborate with	Influence	Inform	Manage/ lead	Deliver to
Internal	Digital Safety Group	✓	✓	✓	✓		✓
	PCVE Programme	✓	✓	✓	✓		
	DIA, including the Policy Regulation and Communities Branch	✓	✓	✓	✓		
External	Minister of Internal Affairs and Cabinet Committees	✓					
	National and international enforcement, security and regulatory agencies	✓	✓		✓		✓
	Christchurch Call	✓	✓	✓	✓		
	Other government departments and agencies	✓	✓		✓		
	Regulatory digital safety system stakeholders	✓	✓		✓		
	Office of Film, Classification & Literature	✓	✓		✓		

Your delegations	
Human Resources and financial delegations	Level Z
Direct reports	Nil
Statutory Powers	Unsolicited Electronic Messages Act 2007 and Films, Videos, and Publications Classification Act 1993 in accordance with the Departmental delegations policy and delegations schedule

Your success profile for this role	What you will bring specifically
At DIA, we have a Capability Framework to help guide our people towards the behaviours and skills needed to be successful. The core success profile for this role is Specialist. **Keys to Success:** • Problem solving • Critical thinking • Interpersonal savvy • Navigating complexity • Communicating with influence • Technical and specialist learning	**Experience:** Experience of CVE/CT, digital and cyber environment, including working with national and international stakeholders • Previous experiences working with international government agencies • Background in intelligence would be beneficial • Experience in developing and supporting the implementation of change processes and building capability • Proven experience in providing professional leadership in an intelligence and CVE/CT environment **Knowledge** • Knowledge of the national and international intelligence communities • Knowledge and experience with machinery of government, including Ministerial briefings • Knowledge of New Zealand's CVE/CT ecosystem and the current digital climate both nationally and internationally • The ability to understand complex situations and to build knowledge and understanding of regulatory and compliance frameworks, functions, and purposes **Skills** • Ability to transfer technical skills and knowledge to managers and staff across different levels • Ability to mentor staff to develop their capability • Excellent relationship management skills to build collaborative relationships to achieve positive results • Ability to influence, lead, and gain the confidence of colleagues and staff • Ability to navigate a complex operating environment and to achieve positive results **Other requirements** • A relevant tertiary qualification

Your success profile for this role	What you will bring specifically
	• Ability to hold and maintain the necessary security clearance. • This position is an Enforcement Officer under the Unsolicited Electronic Messages Act 2007 and an Inspector of Publications under the Films, Videos, and Publications Classification Act 1993