Job description

Haere mai

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

Senior Intelligence Analyst, 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 (digital messaging, child exploitation and violent extremism). 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 be responsible for providing high-quality strategic, tactical and operational intelligence products to Digital Safety while contributing to the development of an innovative, best-practice intelligence function. You will also work closely with partner agencies as part of our intelligence and insights capability to support them.

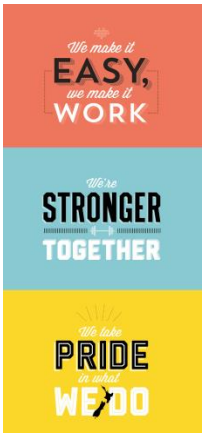
- **Reporting to**: Manager Intelligence and Insights
- **Location:** Wellington
- **Salary range**: Band H (Regulatory)

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.

Spirit of service

Ka mahitahi mātou o te ratonga tūmatanui kia hei painga mō ngā tāngata o Aotearoa i āianei, ā, hei ngā rā ki tua hoki. He kawenga tino whaitake tā mātou hei tautoko i te Karauna i runga i āna hononga ki a ngāi Māori i raro i te Tiriti o Waitangi. Ka tautoko mātou i te kāwanatanga manapori. Ka whakakotahingia mātou e te wairua whakarato ki ō mātou hapori, ā, e arahina ana mātou e ngā mātāpono me ngā tikanga matua o te ratonga tūmatanui i roto i ā mātou mahi.

In the public service we work collectively to make a meaningful difference for New Zealanders now and in the future. We have an important role in supporting the Crown in its relationships with Māori under the Treaty of Waitangi. We support democratic government. We are unified by a spirit of service to our communities and guided by the core principles and values of the public service in our work.

What you will do to contribute	As a result we will see
A trusted senior analyst with knowledge and experience • Conduct analysis of complex digital safety problems by applying recognised methodologies in conducting intelligence analysis and risk profiling. • Draft and present well-reasoned, high-quality intelligence products for decision maker(s) • Lead and produce intelligence product that identifies trends/patterns, risks and opportunities for intervention and prevention. • Brief decision maker(s) on identified trends/patterns, risks and opportunities for intervention and prevention • Deliver intelligence and insight products that contributes to the effectiveness of the business unit • Provide coaching, mentoring and feedback to team members to build capability. • Undertake quality assurance and peer review of the intelligence and analysis work performed by members of the team. • Have an inclusive approach that enables diverse thinking and perspectives to improve the usefulness of intelligence and insights analysis and products to reducing community digital harm • Work with managers to promote effective team work and the sharing of information, insights and intelligence across the business unit.	• Analysis that is intellectually rigorous and operationally sound. • Strong evidence-based information included in well written documents. • The products you and the team produce show evidence of innovation and best practice tools, methodologies and processes. • Team members report positive experiences with coaching, mentoring, and feedback. • Intelligence and information products help to reduce digital harm for iwi, hāpu, and communities across New Zealand. • You can work with and provide analysis/assessment based on ambiguous and incomplete information.
System collaboration and development • Work alongside the Lead Analyst to develop and implement innovative and best practice intelligence, data and information analysis methodologies and processes to support the business unit's regulatory approach to reduce harm • Develop and maintain productive and collaborative relationships across the Department and with external national and international partners. • Proactively engage with partner agencies, sharing and obtaining insights and intelligence information where relevant that ensures reducing community digital harm • Take a system view and utilise customer-centred design practices to enhance the products and	• The Group and our partners can agilely respond to immediate and strategic changes/developments. • An intelligence and data analysis network is maintained across the Department and more widely across government agencies. • Partner agencies and external stakeholders engage in collaborative work that supports communities' outcomes and reduces digital harm. • Partner agencies provide positive feedback about the usefulness of intelligence products received.

What you will do to contribute	As a result we will see
services used by our partner agencies and that help enhance their technical or operational capability. • Participate in internal practice initiatives led by Regulatory Services and wider cross-organisational or sector networks and communities of practice.	• Users of intelligence and insights products report that they met their needs and were communicated with influence through written, verbal and visual mediums. • Your strategic understanding of the system is reflected in your intelligence and insights work.
Responsive and risk-based regulation and stewardship • Identify intelligence and insights related to content, events, organisations and people, across the areas of digital safety, and contribute to minimisation of risks of harm through sharing of intelligence insights. • Assess and manage risks across the various digital safety functions identifying the need for escalation where public safety issues arise. • Collate, identify and analyse risks across digital safety, reporting back to the Operational teams, to give them insight to the more effective use of their resources • Remain up-to-date with developments in intelligence analysis and assessment practice to ensure the intelligence and insights approach and practices remains current. • Use expertise and judgement to understand the intelligence and information needs of the Group and produce quality products that help ensure good outcomes for communities. • Elicit and incorporate stakeholder feedback to maximise the impact of intelligence and information products on regulatory activities. • Facilitate and encourage sharing of information, experience, knowledge and ideas to continue to foster an evidence-based approach where risks of harm are well understood.	• Actionable and timely intelligence and insight products that contribute to the prevention and response work of the Group. • The intelligence and insights products that you produce will enable the Group to collaborate to improve industry responsibility to help keep users safe from digital harm. • The Group's regulatory practice is evidence-based and ensures strategic and targeted use of resources and regulatory activities.
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.	• A safe and healthy workplace for all people using our sites as a place of work. • Health and safety guidelines are followed.

What you will do to contribute	As a result we will see
• 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.	• You can deal successfully with highly stressful environments, including objectionable material (such as child exploitation and violent extremism).

Who you will work with to get the job done		Advise	Collaborate with	Influence	Inform	Manage/ lead	Deliver to
Internal	Digital Safety Group	✓	✓	✓	✓		✓
	DIA, including the Policy, Regulation and Communities Branch	✓	✓		✓		✓
External	Minister of Internal Affairs	✓					
	National and international intelligence enforcement and regulatory agencies	✓	✓		✓		✓
	Other government agencies	✓	✓	✓	✓		
	National and international stakeholders, interest groups, and digital service providers	✓	✓	✓	✓		
	Research communities	✓	✓		✓		

Your delegations	
Human Resources and financial delegations	Z
Direct reports	Nil

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:** • Prior experience in delivering intelligence analysis at strategic and operational levels, in regulatory environments. • Experience in using information systems, information statistical routines and analytical processes. • Experience in environmental scanning and risk assessment, ideally in a regulatory setting so that the underlying drivers of risk(s) to users of digital technology and the causes of harm, such as industry and users' practices, behaviours and attitudes. **Knowledge:** • Knowledge of quantitative and qualitative analysis tools and techniques.

Your success profile for this role	What you will bring specifically
	• Knowledge of the intelligence cycle, and the ability to apply it in the context of government regulatory functions and purpose. • Knowledge of government structures and processes. **Skills:** • Excellent analytical skills. • Excellent oral, visual and written communication skills. • Ability to transfer technical skills and knowledge to managers and staff across different levels. • Ability to mentor staff to help build upon their skills. • Excellent relationship management skills to build collaborative relationships to achieve positive results and to ensure products meet the needs of clients. • Ability to influence and gain the confidence of colleagues and staff. **Other requirements:** • Tertiary qualification in a relevant field and a relevant intelligence-based level of experience from the intelligence career progression framework. • Ability to hold and maintain the necessary security clearance.