

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
-

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 āiane, 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 hāpori, 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
<p>DVE work programme</p> <ul style="list-style-type: none"> • Lead DVE investigations utilising deep knowledge of investigative practices and digital and online environments • Prepare, develop and manage high quality prosecution files including: ensuring prosecution files are completed to an exemplary standard (including full witness briefs and comprehensive exhibit schedules); maintaining and leading input and liaison with Crown Law and assisting direction of Crown Solicitors in prosecution cases; maintaining awareness of legal and technological defences and how to successfully refute; effectively communicating technical issues to judiciary and/or jury; qualifying in Court as an “expert witness” through the delivery of complex testimony • Work with industry partner agencies to remove content that promotes or encourages violent extremism and to identify individuals whose online content indicates a real-world threat to New Zealanders • Monitor national and international current and emerging methods and trends that result in or contribute to serious, harmful content; or behaviours that might improve the effectiveness of DVE investigations • Undertake high quality forensic examinations by: maintaining and applying specialist knowledge of, and training in, data preservation, analysis and presentation; demonstrating high levels of understanding of operating systems and applications including Trojans, spyware, viruses, common file distribution mechanisms, advanced encryption techniques; ensuring the application of internationally recognised and accepted computer forensic methods and procedures in acquisition; creating the forensic construct through internationally accepted acquisition methods; examining, analysing, interpreting and presenting evidence obtained from seized data • Maintain specialist knowledge and latest developments in: <ul style="list-style-type: none"> ◦ computer investigation methodology to detect, preserve, recover and present evidence in relation to DVE investigations ◦ offending and detection (including the rationale, belief systems and language of the groups and individuals engaging in promulgating and promoting violent extremism via digital platforms) 	<ul style="list-style-type: none"> • You lead or contribute to successful investigations that may result in prosecution • The investigations you lead, or support are robust, lawful and safe • You prepare or work with other agencies on affidavits and search warrants • You lead and control crime scenes; ensuring data integrity during search and seizure • You interview offenders and witnesses • Digital Safety and our partners can agilely respond to immediate and strategic developments • You are up to date with and follow best practice detection and investigative techniques • You collaborate with your team and across Digital Safety to explore innovative ideas and approaches and develop them to improve effectiveness • Your colleagues report that you provide flexible support and that you are accountable to one another

What you will do to contribute	As a result, we will see
<ul style="list-style-type: none"> ◦ data preservation and analysis ◦ legal and technological defences and how to successfully refute • Work effectively with diversity, and include diverse people, thinking and perspectives in your work • Provide leadership and coaching with fellow investigators to build capability and share knowledge 	
<p>System leadership and collaboration</p> <ul style="list-style-type: none"> • Develop effective departmental, domestic and international working relationships and alliances to initiate and facilitate consultative processes with key stakeholders • Develop effective working relationships with international enforcement agencies to: <ul style="list-style-type: none"> ◦ facilitate the sharing of information and technological advances; ◦ maximise the business unit’s detection of serious harmful content and behaviours; ◦ and improve our investigative capability • Collaborate within the Department and with national and international agencies to identify, research and develop new initiatives, approaches, and techniques to counter violent extremism 	<ul style="list-style-type: none"> • Increased transparency across the system, including with our partners and across national and international stakeholders and networks • Evidence of collaboration with partner agencies • Your contribution to the development, maintenance and enforcement of all relevant Memorandums of Understanding, directives and guidelines required to support those relationships
<p>Regulation and stewardship targeting responses on a risk and intelligence</p> <ul style="list-style-type: none"> • Identify intelligence and insights related to content, events, organisations and people and contribute to minimisation of risks of harm through sharing of intelligence insights. • Proactively engage in prevention and education activities, by using offender intelligence, identity and detection techniques to investigate and developing an appropriate regulatory response to the harm or risk. • Assess and manage risks associated with violent extremism cases during investigations and prosecutions including identification of the need for escalation where an individual exhibits high risks and public safety issues arise. • Lead the development and implementation of activities with the Online Industry to educate and promote voluntary compliance, raising awareness of Internet safety with the public to reduce public harm and minimise the exposure of harmful content • Undertake DIA’s Online Crisis Response Protocol and the Global Internet Forum to Counter Terrorism Crisis Response by undertaking NZ 	<ul style="list-style-type: none"> • Your regulatory approach is strategically driven and well-informed and you apply a range of tools to detect, investigate and respond to serious, complex, deliberate and harmful content and behaviours • You identify, develop and recommend risk mitigation options and interventions • You contribute to maintaining departmental integrity and you comply with all corporate policies and processes

What you will do to contribute	As a result, we will see
<p>investigative actions to remove harmful digital content after a Terrorism event Contribute to the promotion and effective implementation of changes to policy and procedure</p>	
<p>Health and safety (for self)</p> <ul style="list-style-type: none"> • Monitor, encourage and engage colleagues working with objectionable material to have regular debriefing or counselling to ensure their ongoing well being • Take responsibility for keeping self-free from harm and demonstrate self-awareness to mitigate harm • Participate in the mandated psychological supervision programme and co-operate in implementing the rehabilitation plan • Work safely and take responsibility for keeping self and colleagues free from harm • Report all incidents and hazards promptly • Know what to do in the event of an emergency • Cooperate in implementing return to work plans 	<ul style="list-style-type: none"> • A safe and healthy workplace for all people using our sites as a place of work • All requirements of DIA’s Health and Safety policy and procedures are met including our safe practices for viewing harmful content, and participating in psychological supervision • Acknowledge and manage the impact of our investigation on immediate families and third parties, in a professional manner. • Risks from investigations, interviewing and / or interacting with individuals with extreme belief systems, and carrying out search warrants are managed effectively

Who you will work with to get the job done		Advise	Collaborate with	Influence	Inform	Manage/lead	Deliver to
Internal	Manager Digital Violent Extremism	✓	✓	✓	✓		✓
	Digital Safety	✓	✓	✓	✓		
	Wider staff in DIA	✓	✓	✓	✓		
	Legal Services	✓	✓	✓	✓		
External	Other government departments and agencies	✓	✓		✓		
	Crown Law and Crown Solicitors	✓	✓		✓		
	National and international intelligence, enforcement and regulatory agencies at an operational level	✓	✓		✓		✓
	Office of Film and Literature Classification	✓	✓		✓		
	National and international stakeholders, interest groups, and online service providers	✓	✓		✓		

Your delegations	
Human Resources and financial delegations	Level Z
Direct reports	Nil
Statutory powers	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
<p>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.</p> <p>Keys to Success:</p> <ul style="list-style-type: none"> • Problem solving • Critical thinking • Interpersonal savvy • Navigating complexity • Communicating with influence • Technical and specialist learning 	<p>Experience:</p> <ul style="list-style-type: none"> • Proven experience in leading and conducting complex criminal investigations • Experience in the digital and cyber environment <p>Knowledge:</p> <ul style="list-style-type: none"> • Knowledge of lawful, robust and safe investigative practices, especially in the cyber environment • Knowledge and a sound understanding of regulatory practice • Knowledge of national and international intelligence communities <p>Skills:</p> <ul style="list-style-type: none"> • The ability to prioritize work, ensuring quality and consistency

Your success profile for this role	What you will bring specifically
	<ul style="list-style-type: none">• Advanced understanding of operating systems and applications including Trojans, spyware, viruses, common file distribution mechanisms, advanced encryption techniques and an up to date knowledge of current and new social media sites• Excellent communication skills• Ability to interpret legislation and other technical information• Proven relationship development skills and the ability to be professional, tactful and diplomatic when working with stakeholders and clients <p>Other requirements:</p> <ul style="list-style-type: none">• Ability to hold and maintain Top Secret security clearance• Advanced university degree in law, criminal law, investigation related field or any other relevant subject such as investigation or intelligence, digital forensic, criminal justice, other related area of study such as psychology, sociology, criminology, religion, politics, religion or online investigation, is required. A first level university degree, in combination with two additional years of qualifying experience is accepted in lieu of the advanced university degree.• Are physically able to cope with the physical demands sometimes needed when conducting search warrants and other forms of operational activity and training• This position is an Inspector of Publications for the purposes of the Films, Videos and Publications Classification Act 1993