POSITION DESCRIPTION

Manager Regulatory / Auckland Manager

Unit/Branch, Directorate:	**Regulatory Unit, Information Assurance and Cyber Security Directorate**
Location:	Auckland
Salary range:	K $132,005 - $198,007

Purpose of position: The Manager of the Regulatory Unit is responsible for the oversight and management of national security risk assessments carried out within IACD. The Manager is responsible leading the GCSB team tasked with risk assessments, consultation, and advice associated with TICSA, OSHAA legislation, and other related activities.

The Manager is responsible for the financial forecasting and management, and staff performance and development within the business unit and forms a part of the Directorate Senior Leadership Group with responsibility to develop and deliver Directorate strategic initiatives.

The Manager also has responsibility for the leadership and day to day operation of GCSB Auckland including all its permanent and temporary staff. This management position provides face to face management and leadership for GCSB staff located in Auckland whose line manager is elsewhere.

Our mission at the GCSB is to protect and enhance New Zealand's security and wellbeing

Our values are Respect, Commitment, Integrity and Courage

Information Assurance and Cyber Security Directorate purpose: The IAC Directorate contributes to the national security of New Zealand by providing technical advice and assistance to Government and organisations with significant national information infrastructures to enable them to protect their information from advanced technology-borne threats.

To achieve this, the Directorate provides technical security inspections; high-grade encryption services; information assurance policy and advice; regulation of telecommunications & space activities; and high-end cyber security services to detect and respond to such threats.

Key accountabilities	Deliverables/Outcomes
Manage Auckland Office • Provide efficient and effective leadership and management of the GCSB Auckland (A) administrative and facilities requirements in accordance with published GCSB and other authorised policies and standards • The strategic and policy development of internal GCSB (A) processes • Provide GCSB (A) input into the GCSB strategic and business planning process • Develop and implement effective emergency and health and safety procedures • Ensure all GCSB (A) activities meet the GCSB compliance and legal requirements and policies • Oversee visits to GCSB (A) by internal and external personnel • Ensure the physical security of the Auckland office and staff in accordance with GCSB policies	• All administrative and facilities requirements are met within reasonable timeframes • All provisioning of office services to GCSB (A) business units is undertaken effectively • Emergency planning is adequate and Health and Safety procedures and requirements are communicated, met and complied with • All aspects of office security ensures that no unauthorised access is gained to classified areas or information and physical barriers
Developing and managing people • Effectively lead, develop and manage staff and positively influence their progress towards successful results • Effectively manage workloads to ensure they are equitable • In conjunction with People Capability, address poor performance of employees and ensure that good conduct and discipline is maintained at all times and any issues are dealt with promptly • Demonstrate the stated values of the organisation in all aspects of their representation of the team/Bureau • Ensure performance objectives, reviews and discussions are completed in line with Bureau policies and procedures for all direct reports • Conduct regular team meetings to share information and update staff on new requirements and policies • Support individual team leaders to achieve objectives, identify personal development opportunities, recognise areas of improvement and establish solution based outcomes • Ensure effective recruitment to attract the best person for the position and then	• Each team member understands clearly what is required of them and receives regular constructive feedback on progress • Each team member understands their contribution to Bureau outputs • Performance reviews are completed thoroughly and forwarded to People Capability within specified timeframes • Employees have a training and development plan that is carried out in conjunction with People Capability • Employees understand and demonstrate Bureau values in their day to day work • Employee issues (including non-performance issues) are successfully addressed in a timely manner • Leave liability is kept at a reasonable level • Staff are fully informed on relevant information, and organisational policies and procedures are complied with • New staff are comprehensively inducted so that they are productive and comfortable in their role within 3 months • Auckland based staff with no local line management are appropriately managed by proxy

ensure a complete and comprehensive induction takes place	
Contribute to the execution of the IACD Operational Plan • Promoting cross-team collaboration through the execution of the IACD Operational Plan and support for operational exchanges between different IACD business units • Participating in both functional (specific skill-sets) and cross-functional (mixed skill-sets) IACD teams at the request of the IACD Executive Team and Leadership Group • Pro-actively demonstrating a willingness to transfer skill sets to other teams in times of operational surge and crisis • Making a constructive contribution to the execution of the Operational Plan	• Team silos are visibly reduced and the focus of staff shifts from their own unit plan to delivering Directorate-wide objectives • Customer feedback suggests that the plan is having a positive effect on IACD's performance through the creation of a more obviously joined-up operating model • Policy and process gaps, which negatively affect IACD operations, are highlighted and rectified • Staff retain an active interest in developments within IACD beyond their normal area of operation • Specific measure: active participation in at least one Operational Plan Working Group; a positive response to Senior Leadership requests for assistance beyond day-to-day responsibilities
Business and financial planning • Manage and maintain the Unit's annual budget in accordance with GCSB Finance Instructions. Report monthly on any variances to the Finance business unit • Unit business plans are developed to enhance the capability and outputs of the Unit • Unit business plans are clearly communicated to the team and inform individual performance objectives	• Budget spent in accordance with financial authority and instructions • Variances reported • Business plans are completed within required timeframes and comply with GCSB planning templates (where available) • Supervisors and staff understand how their work and outputs contribute to the business plan • Business plan objectives are reflected in all individual performance plans
Delivery of GCSB obligations under the TICSA • Manage TICSA national security risk assessment process • Approve TICSA national security risk assessments under delegation from Director GCSB • Ensuring all unit members understand and comply with their legal and compliance obligations • Ensure close collaboration with other GCSB units and partner agencies to ensure complete and timely information contribution towards risk assessments • Ensure all unit output meets legislative requirements	• Potential threats to NZ national security resulting from planned changes within network operator infrastructure are identified and sufficiently mitigated • Any assessment decisions that are challenged withstand scrutiny • Communications with NZ network operators both proactively and reactively are done so in accordance with all relevant legislation

• Ensure all unit outputs meets customer requirements	
Delivery of GCSB obligations under the Out of Space High Altitude Activities (OSHAA) • Manage GCSB OSHAA national security risk assessment process • Approve GCSB OSHAA national security risk assessments for inclusion into NZIC assessment and recommendation findings • Ensuring all unit members understand and comply with their legal and compliance obligations • Ensure close collaboration with other GCSB units and partner agencies to ensure complete and timely information contribution towards risk assessments • Ensure all unit output meets legislative requirements and are incorporated into NZIC output	• GCSB and MBIE executive are appraised of potential national security concerns early • Launches not delayed due to unexpected or avoidable delays caused by GCSB • Any assessment decisions that are challenged withstand scrutiny
Health and safety (for self) • 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 • Be a **visible** role model at all times • **Follow** GCSB's safety rules and procedures **Health and safety (for team):** • Inform, train and equip staff to carry out their work safely • Ensure prompt and accurate reporting and investigation of all workplace incidents and injuries • Assess all hazards promptly and ensure they are managed	• A safe and healthy workplace for all people using our sites as a place of work • All requirements in the NZIC Health and Safety policy and procedures are met
Other duties	Any other duties that fall within the scope of the position

Position delegation	
Financial delegation:	None

Key stakeholders	
Internal:	• NZIC staff at all levels.
External:	• New Zealand Government agencies • Collaborating international Information Assurance agencies and government agencies, authorities and organisations • Telecommunications network operators (approx. 160), service providers and equipment manufacturers • High Altitude vehicle operators and suppliers

Person Specification	
Experience:	• Previous experience of 7 or more years at a management level in the use of human, technical, and financial resources • A minimum of 10 years relevant experience in the New Zealand telecommunications sector • Experience in the application and management of telecommunications and information system security technologies and countermeasures to exploitation • Programme or project management experience • Experience in the development and management of policy and plans at a corporate level • Previous successful experience in managing a team of experts • Extensive operational experience in the application of information assurance or security techniques and countermeasures, or intelligence collection and operations • Experience managing stakeholder or client relationships
Knowledge and Skills:	• A thorough understanding of contemporary telecommunications technology • Knowledge and experience in regulatory processes, policy advice and compliance frameworks • Highly developed oral and written communication skills, including the ability to communicate and build relationships at all levels • Highly developed negotiation, advocacy, influencing and relationship management

	skills • Strong interpersonal and communication skills, and the ability to relate effectively to both technical and non-technical people • The ability to represent the GCSB with credit within national and international communities • An eye to detail and a commitment to accuracy and quality in all work activities • Proven leadership qualities in a technical environment, and the ability to deal effectively and sensitively with other people
Qualifications and Courses:	• Tertiary level qualification (Bachelor level) or equivalent experience, in Information Technology, Computer Science or equivalent, with an emphasis on information security • Tertiary papers in computer science and information security • Master's degree in any field. • Current CISSP or CISM or other equivalent professional computing/networking qualification
Specialist Competencies: *This list contains what is required for the 100% fully effective level.*	• Telecommunications networks • IA expert knowledge • Regulatory enforcement • Formulate and implement policy • SIGINT Access and exploitation • Relationship management • Computer network exploitation • IT security policies • Risk management • Network security management • Consultancy knowledge • Database administration • Business communications • Computer network defence
Specific Job Requirements:	• Ability to obtain and maintain a TSS security clearance

NZIC Competencies

In addition to the Person Specification above, competency standards which outline the development requirements of the position are set out under the NZ Intelligence Community (NZIC) Career Pathways framework. The Career Pathways framework enables progression within the job.

Full descriptions of progression competencies and an overview of the NZIC Career Pathways framework is available on appointment.

The position is aligned to the People Leader competency framework.

Diversity and Inclusion

The GCSB and NZSIS recognises that our success requires us to have a workforce that reflects the community we serve and diversity in its widest context – where all people, regardless of difference are valued and respected.

One way we show our inclusion of those with diverse sexual and gender identifies is with a Rainbow Tick accreditation which we proudly received in 2019.

We are committed to building a workplace where we can say we have achieved – ***He waka eke noa*** – a canoe which we are all in with no exception.

Changes to Position Description

Positions in the GCSB may change over time as the organisation develops. Therefore we are committed to maintaining a flexible organisation structure that best enables us to meet changing market and customer needs. Responsibilities for this position may change over time as the job evolves. This Position Description may be reviewed as part of planning for the annual performance cycle.

Date PD reviewed: 10/08/2018

Signatures		
Manager's Name		
Signature		Date:

Employee's Name		
Signature		Date: