Position Description

GCSB Manager, Mission Enablement (ME)

| Business unit: | Mission Enablement  
|              | Information Assurance and Cyber Security Directorate (IACD) |
| Responsible to: | Deputy Director, Information Assurance and Cyber security Directorate |
| Position purpose: | As part of the IACD Executive Team and Leadership Group, Manager, Mission Enablement (ME), is responsible for reducing harm to vital New Zealand information infrastructures by ensuring that IACD has the people, resources, facilities, operating environment, relationships and reputation needed to discharge its operational role. |

The Manager, Mission Enablement assists DDIAC in the development, refinement and execution of the IACD vision, core goal, strategy and operational plan.

The ME Manager plays a key role in facilitating the delivery of IAC services to customers by providing the day to day oversight of the Directorate’s human resources, financial, logistics, communications and other mission enablement functions.

The ME Manager is responsible for the performance and output of the Mission Enablement team tasked with the responsibility to maintain and enhance IACD’s relationships and national profile through effective strategic communications, recruitment and policy work. The ME Manager’s role also encompasses delegated responsibility from DDIAC when necessary.

Direct reports: 4
Financial delegation: Level 4

Directorate overview: The IAC Directorate contributes to the national security of New Zealand by providing technical advice, assistance and protection 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 cryptographic and high assurance services; information assurance policy and advice; and high-end cyber security services to detect and respond to such threats.

Business unit overview: The Mission Enablement and Strategic Communications Cell is responsible for reducing harm to New Zealand’s vital information infrastructures by ensuring that IACD has the people, facilities, operating environment, relationships and reputation needed to discharge its operational role. It does this by:

- leading on strategic communications issues for IACD, both internally and externally, including through the provision of: UNCLASSIFIED statistics, metrics and trend reporting; support to seniors (e.g. speeches, interviews and talking points); and reputation management;
- enhancing the external standing of IACD through customer-oriented management of the online interface between the Directorate and the public and by maintaining associated web-content;
- providing technical advice to customers that is clear, consistent, relevant and frequently updated;
- collaborating closely with other NZ government agencies, NGOs, academia and security professionals to ensure that messaging on Information Assurance and Cyber Security is reliable and timely;
- supporting ‘one-to-many’ external engagement on Information Assurance and Cyber Security topics and assisting the Outreach and Engagement Management team in their customer-specific and sectoral engagement;
- coordinating the practical requirements of IACD’s expansion including recruitment and retention; training and development; accommodation, environmental and financial issues;
- managing the implementation of the IACD operational plan designed to create the future IACD operating model;
- designing and implementing a metrics system that enables IACD to assess the impact it is having in reducing harm to New Zealand’s vital information infrastructures.
<table>
<thead>
<tr>
<th>Remuneration indicator:</th>
<th>Ribbonwood pay band J</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date evaluated:</td>
<td>May 2015</td>
</tr>
</tbody>
</table>
GCSB mission and values

Our mission
Protecting and Enhancing New Zealand’s Security and Wellbeing.

Our values
Respect, Commitment, Integrity, Courage.

IACD directorate mission, values and goal

Our vision
Protect New Zealand’s vital information infrastructures.

Our mission
To be a team of confident professionals, admired for our innovation and regarded both domestically and internationally as leaders in the Information Assurance and Cyber sectors.

To have a comprehensive understanding of advanced technology-borne attempts to target our vital information infrastructures and steal our secrets and intellectual property.

To be confident about our ability to monitor these threats and either reduce harm directly through timely provision of assurance and technical services or help others to mitigate risks through authoritative policy and expert advice built on our unique capabilities.

Our goal
There are no advanced technology-borne compromises from the most significant national infrastructures by June 2016.
Functional relationships

External contacts:
- Domestic Partner Agencies
- International Partner Agencies
- NZ Information Assurance Customers
- Contractors
- NCPO
- Private and Public sector

Internal contacts:
- DDIAC
- AD Operation, AD Projects, IACD Exec team
- IAC Directorate staff
- ICSS staff
- People capability staff
- Project team members
- Protective Security Enablement team
- Logistics staff
- Other GCSB/NZSIS staff as necessary

Objectives

The position of ME Manager encompasses the following major functions or objectives:

- Operational Plan and Theory of Change
- Developing and management of staff
- Reputation and relationship management
- External presentation of the Directorate, including publications and recruitment
- Business management, financial oversight and projects to accommodate growth
- Deputising for DDIACD and ADs on all non-operational matters affecting the Directorate

The requirements in the above objectives are broadly identified below:

<table>
<thead>
<tr>
<th>Jobholder is accountable for:</th>
<th>Jobholder is successful when:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operational Plan and Theory of Change</strong></td>
<td><strong>IACD is able to demonstrate that the Directorate's actions are visibly contributing towards the reduction of harm.</strong></td>
</tr>
<tr>
<td>Devising and implementing a system to measure IACD's impact with its customers</td>
<td><strong>Customer feedback suggests that the plan is having a positive effect on IACD's performance through the creation of an improved operating model</strong></td>
</tr>
<tr>
<td>Sharing responsibility for the delivery of the IACD Operational Plan for 2014-2016.</td>
<td><strong>Contributing through participation in cross-functional IACD teams to the development, refinement and execution of the plan</strong></td>
</tr>
<tr>
<td>Making a constructive contribution to discussions on the execution of the plan.</td>
<td></td>
</tr>
<tr>
<td>Providing honest feedback on the future refinement of the plan.</td>
<td></td>
</tr>
<tr>
<td>Playing a proactive role as a member of the IACD Executive</td>
<td></td>
</tr>
</tbody>
</table>
Team.

- Behaving as a leader within and outside of the unit; embodying the Bureau's values.
- Oversee implementation, monitoring and strategic review of the IACD operational plan (2014-2016); ensure that successor documentation is in place from July 2016 onwards.
- Contribute to the development and maintenance of ME Unit procedures.
- Promote cross-team collaboration through the execution of the IACD Operational Plan and support for operational exchanges between different IACD business units.
- Participate 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.

Developing and Managing Staff

- Effectively lead, develop and manage unit staff and positively influence their progress towards successful results.
- Effectively manage workloads to ensure they are appropriate to meet Unit objectives and staff abilities.
- 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

- Confident about and responsible for proposing amendments to the plan and ensuring that they are enacted.
- Policy and process gaps, which negatively affect ME operations, are highlighted and rectified.
- Team silos are visibly reduced and the focus of staff shifts from their own unit plan to delivering Directorate-wide objectives.
- 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 ET/LG requests for assistance beyond day-to-day responsibilities.

- Staff are motivated and engaged with a clear understanding of the technical requirements that meet unit and organisational objectives
- Staff and unit workloads are managed to ensure:
  - Unit priorities are and outcomes are met
  - Staff are fully employed commensurate with their individual level
  - Unit and staff performance is continuously monitored
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 staff 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 ensure a complete and comprehensive induction takes place.

■ Ensure a training program is designed and implemented for all staff. Oversight of IACD Development Plans and training in conjunction with L+D.

■ The Unit is kept appraised on a regular basis with clear and open sharing of appropriate information.

■ Supervisory and other leadership staff are developed with succession in mind and to ensure the continued stability and success of the Unit.

■ Appropriate staff are recruited with induction obligations met and signed off.

■ Staff are appropriately trained to meet Unit objectives.

■ Unit is performing to its expected potential.

Reputation and relationship management
Develop and enhance the IAC Directorate’s reputation and image by:

■ Leading the Directorate’s relationship with ICSS, particularly OD+P and Finance.

■ Promoting the establishment and maintenance of productive relationships within the Directorate and between the IACD and the wider

■ IACD is regarded as a close partner of ICSS’s; issues are aired quickly, constructively and calmly; IACD officers contribute willingly to corporate initiatives and appreciate their significance for their day-to-day roles.

■ The IAC Directorate is able to function with any variance addressed fairly and within an appropriate timeframe.

- Organisational values are represented appropriately and respectfully.

- Performance management obligations are completed within published schedules.

- Recommendations for improvement and staff development opportunities are considered.

- Oversight of IACD Development Plans and training in conjunction with L+D with any variance addressed fairly and within an appropriate timeframe.

- Organisational values are represented appropriately and respectfully.

- Performance management obligations are completed within published schedules.

- Recommendations for improvement and staff development opportunities are considered.
Bureau.

- Promoting the establishment and maintenance of good relationships between the IAC Directorate and other Government agencies
- Promoting the establishment and maintenance of good relationships between the IAC Directorate and 2nd Party agencies
- Oversight of strategic communications engagement on cyber security communications
- Oversight of reputational management with Mission Enablement and IACD as a whole.
- Oversight of inter-agency collaboration on cyber-security related topics, including with DIA/GCIO, NCPO and MBIE

**External presentation including publications and recruitment**

- Formulating new business processes in order to enhance service delivery, where need is identified;
- Provide oversight of IACD Cyber Reporting team and Strategic communications to action and dissemination of CLASSIFIED reporting at the most practical and usable level. Additionally, to ensure that a consistent standard is reached in our Outputs.
- Managing the communications support to IAC business in collaboration with the IACD Comms Officer often working on complex, multi-faceted programs
- Managing the co-ordination of the IACD intranet web page design and update services.
- Management of projects that

and collaborate across all parties with the minimum of friction and maximum co-operation.

- IACD has a constructive relationship with ID and works together with the Directorate to develop attractive transferable and stimulating careers that bridge both the ‘defensive’ and ‘offensive’ missions of the Bureau.
- IACDs customer survey scores demonstrate noticeable improvement; partners comment on our more collaborative approach.
- IACD officers contribute creatively and willingly to Bureau-wide initiatives

- The desired aim is achieved within specified timeframes and financial constraints
- Project documentation is completed and filed.
- Recruitment is prioritised and campaigned result in the successful hiring of high quality candidates
contribute to the fulfilment of the IACD mission.

- Oversight of Strategic communications publications and non-technical recruitment
- Acting as a central point of coordination for large-scale IACD recruitment campaigns.
- Managing other projects as directed, utilising project management principles and processes,

**Business management, financial oversight and projects**

- Manage and maintain the Unit’s annual budget in accordance with GCSB Finance Instructions. Report monthly on any variances to the Finance business unit.
- Acting as Controlling Officer for the ‘Line 30’ Directorate budget under AD / DDIAC’s authority (2014/15 budget = 450k)
- Oversee management of IACD-wide risks and risk reporting.
- Oversee IACD budgetary inputs to the GCSB’s budget formulation process.
- Managing Accommodation both in PHOP and in Auckland to accommodate growth
- Managing other projects as directed, utilising project management principles and processes
- Unit financial obligations are met within GCSB financial instructions and the Budget spent in accordance with financial authority.
- Unit business plans are developed, monitored, and adjusted to ensure unit meets GCSB expectations.
- Business growth opportunities are identified, evaluated, and recommended appropriately.
- Supervisors, team leaders and staff understand how their work and outputs contribute to the Business Plan.
- Business Plan objectives are reflected in all individual performance plans.
- Unit objectives compliment NCSC objectives, and the NCSC operates as a cohesive whole.
- Problem areas are resolved to DDIAC and ADs’ satisfaction
- Process improvements are identified and implemented; Outputs all reach a common standard endorsed by DDIAC.
- Requested communications support is provided to the customer’s
Deputising on all non-operational matters affecting the Directorate

Fostering an environment where DDIAC or ADs can focus on issues of strategic significance by:

- Acting as a link on staffing matters between DDIAC / IACD ADs and Unit Managers.
- Taking on delegated responsibility for DDIAC, such as attending meetings, writing Board papers, Ministerial briefings and representation with customers.
- On DDIAC's behalf, maintaining oversight of IAC Directorate personnel matters and on specific direction by AD Ops and DDIAC, becoming actively involved in personnel issues where necessary.
- deputising for DDIACD and ADs at Board; Prayers; Staffing Committee; leading on difficult HR issues relating to Performance and behaviour; Quality Assurance oversight of all non-operational external products from the Directorate.

- IAC Intranet web pages are relevant and up to date.
- IACDs senior managers' time spent on strategic issues is optimised.
- Staffing issues are resolved wherever possible between Unit Managers, the Business Manager and ICSS.
- IACD develops successful and consistent ways to record and assess how the Directorate adds value. [NB: this is particularly challenging task – the Directorate has a multitude of different inputs, outputs and customers to aggregate in any metrics it uses. Establishing the IACD value proposition requires high-end problem-solving skills and real creativity.

Precise performance measures for this position will be developed in discussion between the jobholder and manager as part of the performance development and review process. It is also expected that you will undertake other duties that can be reasonably be regarded as relevant to the position, your experience and capability.

Person specification

This section is designed to capture the expertise required for the role at the 100% fully effective level. (This does not necessarily reflect what expertise the current jobholder has.) This may be a combination of knowledge, experience, key skills, attributes, job specific competencies, qualifications or equivalent level of learning.
## Qualifications

<table>
<thead>
<tr>
<th>Essential</th>
<th>Desirable</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ Tertiary qualification in Business studies or equivalent work experience</td>
<td>■ A background or interest in IT Security or Communications Security</td>
</tr>
<tr>
<td>■ An understanding of the NZIC</td>
<td>■ An understanding of the NZIC</td>
</tr>
</tbody>
</table>

## Knowledge/experience

<table>
<thead>
<tr>
<th>Essential</th>
<th>Desirable</th>
</tr>
</thead>
<tbody>
<tr>
<td>■ Ideally 10+ years’ relevant experience, preferably within the NZIC. The job requires experience of a broad nature along with an awareness of work activities beyond the immediate job situation and the impact of the job on these activities and the ability to work in harmony with conflicting and diverse activities.</td>
<td>■ At least 5 years’ experience in IT security or network defence.</td>
</tr>
<tr>
<td>■ Experience in Financial, technical and human resource Management.</td>
<td>■ A well-developed understanding of the business of the IAC Directorate combined with the knowledge of how best to focus the support activities necessary to optimise the Directorate’s mission.</td>
</tr>
<tr>
<td>■ Effective communications skills and an ability to engage with people at all levels of the Bureau and in other Government agencies.</td>
<td>■ Good GCSB Organisational Knowledge.</td>
</tr>
<tr>
<td>■ Experience at a management level in the use of human, technical, and financial resources.</td>
<td>■ The ability to identify and resolve highly complex issues in an environment where there may be little or no prior guidance.</td>
</tr>
<tr>
<td>■ Experience in the development and management of policy and plans at a corporate level.</td>
<td>■ The ability to conceptualise and develop innovative solutions.</td>
</tr>
<tr>
<td>■ Highly developed communication, negotiation and relationship management skills.</td>
<td>■ An understanding of the IT security</td>
</tr>
</tbody>
</table>
industry and the machinery of government.

**Personal attributes**

- Enthusiasm, self-motivation and innovation.
- Demonstrate sound judgment, tact and integrity in dealing with complex or sensitive issues.
- Displays initiative and self-confidence.
- The resilience to operate under pressure and correctly identify and assess risk, and make justifiable operational decisions.
- Proven leadership qualities in a technical environment, and the ability to deal effectively and sensitively with other people.
- Highly effective planning, management and organisational skills.
- Highly developed oral and written communication skills, including the ability to communicate and build relationships at all levels; and to maintain a courteous, diplomatic and personable approach to customers and community partners.
- The ability to participate in management forums as an effective member of the team, and contribute to the development of a high performance organisation.
- The ability to effectively represent the GCSB within national and international communities.
- Ability to build productive relationships with customers and stakeholders.

**Core competencies**

*Core competencies are based on and consistent with our values. They describe qualities that are common requirements for all GCSB staff at differing levels in the organisation, irrespective of their specialist skills or the particular requirements of their job. They are complemented by specialist competencies, which (where applicable) are set out in individual performance agreements.*

All employees are measured against the following core competencies as part of performance development and review:

- Security
- Teamwork and leadership
- Results focus
- Communication and knowledge sharing
- Professionalism
- Innovation
- Customer focus

In addition collaboration in the New Zealand Intelligence Community is critical for success in GCSB roles. Employees will also be measured against their ability to work together in the NZIC to achieve outcomes.
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. Such change may be initiated as necessary by the manager of this position. This position description may be reviewed as part of planning for the annual performance cycle.

Health and safety

GCSB is committed to providing a healthy and safe work environment and management practices for all employees. Employees are expected to share this commitment as outlined in the Health and Safety in Employment Act by taking all practicable steps to ensure:

- The employee's safety while at work; and
- That no action or inaction of the employee while at work causes harm to any other person.

Knowledge management

Employees are responsible for ensuring that all business records created are accessible and stored in the correct manner according to GCSB record keeping policy, standards, and procedures.

Employee: ___________________________ Date: ___________________________

Manager: ___________________________ Date: ___________________________