GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

# POSITION DESCRIPTION

## Cyber Threat Analyst

| | |
|---|---|
| **Unit/Branch, Directorate:** | Cyber Threat Response (CTR)<br>Information Assurance and Cyber Security Directorate |
| **Location:** | Wellington |
| **Direct reports:** | Nil |
| **Salary range:** | H $77,711 - $116,567 |

---

**Purpose of position:** The Cyber Threat Analyst's role works to understand the cyber threat environment and provides insights through a range of outputs to help inform a range of stakeholders, including domestic NCSC customers, New Zealand government agencies and partner agencies.

---

**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 |
|---|---|
| **Understanding the cyber threat environment**<br>• Maintaining an understanding of the cyber threat to New Zealand.<br>• Maintaining an understanding of attack tool capabilities and infrastructure.<br>• Maintaining and improving technical awareness and literacy regarding cyber threats and forensic analysis. | • GCSB remains aware of cyber threat actors' intentions and capabilities, and the CTR Unit remains aware of the current computer network defence (CND) trends and how these might impact New Zealand.<br>• NCSC remains the point of contact as the area of cyber security expertise and knowledge within New Zealand.<br>• The CTR Unit retains a high standard of research and analysis of cyber threats. |
| **Cyber Threat Analysis**<br>• Lead the analysis of multi-source evidence to maintain awareness of cyber events and electronic attacks.<br>• Collect, collate and analyse cyber security events, incidents and investigative leads.<br>• Prepare, document, and maintain event reports, requests to/from customers, and contribute to the development of policy statements as required.<br>• Manage personal tasking, and remain aware of Unit-wide operational developments, to ensure timeliness and deliverables.<br>• Develop, maintain, and improve technical understanding and analytic techniques. Provide briefings and accounts of these analytic techniques to colleagues, as appropriate. | • The capabilities and intentions of adversaries are clearly understood.<br>• Analytic observations or answers enable GCSB to provide an enhanced CND service.<br>• The risk to New Zealand infrastructure is understood.<br>• Cyber security events are recorded, evaluated and responded to in a timely and efficient manner.<br>• The escalation of an incident, and initiation of an investigative response, is based on well documented decision making and event reporting.<br>• Briefings and reports are appropriately constructed and delivered to ensure a consistent and an accurate message is delivered to all stakeholders. |
| **Delivery of output**<br>• Produce timely and relevant cyber security related reporting for customers, based on material obtained from CND systems, intelligence partners, and unclassified sources.<br>• Enhance GCSB's relationships and reputation with customers and partners through professional representation and engagement. Ensure output capabilities and limitations are known to customers where appropriate.<br>• Communicate effectively with technical, legal, executive, and leadership teams within GCSB, and within external customer and partner agencies. | • CTR Unit provides timely and accurate technical advice and expertise.<br>• The content of CTR Unit's technical reporting and advice is unambiguous, and the implications of why it has been provided are clear.<br>• Team product meets all required quality standards, as specified in relevant policy documentation.<br>• Team product does not violate compliance rules, and any inadvertent breaches are notified to Compliance and dealt with appropriately.<br>• Productive and enduring relationships are formed with domestic and international partners. |

| | |
|---|---|
| | • CTR Unit has a detailed awareness of customers' needs and expectations.<br>• Customer and partner enquiries are attended to in a timely manner. |
| **Contribute to the execution of the IACD Strategic Plan**<br>• Promoting cross-team collaboration through the execution of the IACD Strategic Plan and support for operational exchanges between different IACD business units.<br>• 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.<br>• Pro-actively demonstrating a willingness to transfer skill sets to other teams in times of operational surge and crisis.<br>• Making a constructive contribution to the execution of the IACD Strategic Plan. | • Team silos are visibly reduced and the focus of staff shifts from their own Unit Plans to delivering Directorate-wide objectives.<br>• Customer feedback suggests the Strategic Plan is having a positive effect on IACD's performance through the creation of a more obviously joined-up operating model.<br>• Policy and process gaps, which negatively affect IACD operations, are highlighted and rectified.<br>• Staff retain an active interest in developments within IACD beyond their normal area of operation. |
| **Health and safety (for self)**<br>• Work safely and take responsibility for keeping self and colleagues free from harm.<br>• Report all incidents and hazards promptly.<br>• Know what to do in the event of an emergency.<br>• Cooperate in implementing return to work plans.<br>• Be a **visible** role model at all times.<br>• **Follow** GCSB's safety rules and procedures. | • A safe and healthy workplace for all people using our sites as a place of work.<br>• 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: | • IACD teams primarily and the GCSB more generally |
| External: | • New Zealand government agencies, along with NCSC customers domestically.<br>• A range of international partnerships and cyber security forums. |

| Person Specification | |
|---|---|
| Experience: | • A background in intelligence analysis, cyber security or information assurance.<br>• A good understanding of intelligence production and delivery mechanisms, especially with regard to CND product. (desirable) |
| Knowledge and Skills: | • Excellent written communication skills and an ability to analyse and summarise data.<br>• Presentation, public speaking or training skills and experience. |
| Qualifications and Courses: | • A tertiary qualification incorporating Computer Security study and/or equivalent experience; OR<br>• A tertiary qualification or equivalent experience incorporating technical analysis, problem solving, and report writing. |
| 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.

## 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: 21/06/2018

| **Signatures** | | |
|---|---|---|
| Managers Name | | |
| Signature | | Date: |

| | | |
|---|---|---|
| Employee's Name | | |
| Signature | | Date: |