CENTRELINK FRAUD CONTROL PLAN 2008-2010

Australian Government

Centrelink
giving you options

To All Employees

Centrelink's core values include accepting responsibility for what we do, and conducting our business in a transparent manner. As Chief Executive Officer, it is my duty to ensure Centrelink is accountable for its actions.

Each year, Centrelink distributes over $63 billion of public money in payments on behalf of more than 20 organisations. We have clear obligations under the *Financial Management and Accountability Act 1997* to have in place effective planning, risk management, audit and financial management processes. My role is to ensure the effective and efficient use of Centrelink's resources and that the integrity of programs delivered by Centrelink is not compromised.

The *Centrelink Fraud Control Plan 2008-10* sets out our commitment to fraud control and business integrity for the next two financial years. The fraud control strategy outlined in the Plan provides an integrated approach to delivering business integrity outcomes through a focus on prevention, detection and deterrence of fraud. Where prevention fails, we need effective detection of fraud, so that investigations can be undertaken, debts recovered and prosecutions initiated where appropriate.

Our collective responsibility is to ensure fraud and business integrity risks are identified and addressed. We must be committed individually to the highest ethical standards through our values and behaviours.

I ask that you carefully read the plan so that you understand your role in ensuring the integrity of outlays on behalf of the Government and all Australians.

Carolyn Hogg
A/g Chief Executive Officer

Table of Contents

EXECUTIVE SUMMARY 6
1. ABOUT CENTRELINK'S FRAUD CONTROL PLAN 7
1.1 OVERVIEW 7
1.2 CENTRELINK'S STRATEGIC DIRECTIONS 7
2. FRAUD CONTROL RESPONSIBILITIES 8
2.1 WHAT ARE CENTRELINK'S STANDARDS FOR EMPLOYEES AS THEY RELATE TO THE FRAUD CONTROL PLAN? 11
2.1.1 INTEGRATED LEADERSHIP SYSTEM (ILS) 11
2.1.2 AUSTRALIAN PUBLIC SERVICE CODE OF CONDUCT AND VALUES 11
2.1.3 INFORMATION TO EMPLOYEES 11
2.1.4 CHIEF EXECUTIVE INSTRUCTIONS 12
2.2 HOW DOES CENTRELINK PROTECT ITS EMPLOYEE AND CUSTOMER INFORMATION? 13
2.2.1 PHYSICAL SECURITY 13
2.2.2 PERSONNEL SECURITY 13
2.2.3 INFORMATION AND COMMUNICATIONS TECHNOLOGY SECURITY 14
3. WHAT IS FRAUD CONTROL? 15
3.1 DEFINITION OF FRAUD 15
3.2 FRAUD IN CENTRELINK 15
3.3 FRAUD CONTROL IN CENTRELINK 16
4. ABOUT CENTRELINK 17
4.1 OVERVIEW 17
4.2 NATIONAL SUPPORT OFFICE 17
4.2.1 THE CHIEF EXECUTIVE OFFICER 17
4.2.2 CHIEF FINANCIAL OFFICER- FINANCE DIVISION 18
4.2.3 CORPORATE IT SYSTEMS DIVISION 18
4.2.4 FAMILIES, SENIORS AND BUSINESS INTEGRITY DIVISION 18
4.2.5 PEOPLE AND MINISTERIAL DIVISION 19
4.2.6 AUDIT, GOVERNANCE AND ASSURANCE DIVISION 19
4.3 CUSTOMER SERVICE DELIVERY 20
4.3.1 AREA NETWORK 20
4.3.2 CUSTOMER SERVICE NETWORK 20
4.3.3 CUSTOMER SERVICE SUPPORT CENTRES 20
4.4 CENTRELINK ORGANISATIONAL STRUCTURE & STRATEGIC COMMITTEE FRAMEWORK 21
5. WHAT DO THE COMMONWEALTH FRAUD CONTROL GUIDELINES MEAN FOR CENTRELINK? 23
5.1 OVERVIEW 23
5.2 REPORTING 24
5.2.1 OTHER REPORTING 24
5.3 RESPONSIBILITIES 25
5.3.1 THE COMMONWEALTH DIRECTOR OF PUBLIC PROSECUTIONS 25
5.3.2 THE ATTORNEY-GENERAL'S DEPARTMENT 25
5.3.3 THE AUSTRALIAN FEDERAL POLICE 25
5.4 FRAUD CONTROL PLANNING 26
5.5 FRAUD CONTROL TRAINING 27

5.6 RISK MANAGEMENT....27
5.6.1 FRAUD RISK ASSESSMENTS....28
5.7 REPORTING FRAUD TO CENTRELINK....29
5.8 REPORTING FRAUD WITHIN CENTRELINK....29
6. FRAUD PLAN FOR PAYMENT RISKS....30
6.1 OVERVIEW....30
6.1.1 PAYMENT FRAUD MANAGEMENT FRAMEWORK....31
6.2 PAYMENT RISK MANAGEMENT....32
6.3 PERFORMANCE MONITORING AND QUALITY ASSURANCE....32
6.4 KEY RISKS....33
6.5 CONTROLLING PAYMENT RISK - STRATEGIES AND ACTIVITIES TO PREVENT PAYMENT INACCURACY (INCLUDING FRAUD)....34
6.5.1 BUSINESS INTEGRITY STRATEGY....34
6.5.2 GETTING IT RIGHT....35
6.5.3 TIERED PROOF OF IDENTITY MODEL....35
6.5.4 DEBT SERVICING....36
6.5.5 INFORMATION TO CUSTOMERS....36
6.5.6 INFORMATION TO EMPLOYEES....37
6.5.7 EDUCATION AND TRAINING OF EMPLOYEES....37
6.6 STRATEGIES AND ACTIVITIES TO DETECT PAYMENT INACCURACY (INCLUDING FRAUD)....37
6.6.1 COMPLIANCE REVIEWS....37
6.6.2 SERVICE PROFILING....38
6.6.3 ANALYSIS....38
6.6.4 INVESTIGATIONS....38
6.6.5 FRAUD INTELLIGENCE....38
6.6.6 IDENTITY CRIME....39
6.6.7 OUTPOSTED AUSTRALIAN FEDERAL POLICE AGENTS....40
6.7 STRATEGIES AND ACTIVITIES TO DETER PAYMENT FRAUD....40
6.7.1 MEDIA EXPOSURE....40
6.7.2 DEBT RECOVERY....41
6.7.3 PROSECUTIONS....41
7. FRAUD PLAN FOR ADMINISTRATIVE AND STAFF FRAUD RISKS....42
7.1 OVERVIEW....42
7.1.1 ADMINISTRATIVE AND STAFF FRAUD MANAGEMENT FRAMEWORK 43
7.2 KEY RISKS....44
7.3 STRATEGIES AND ACTIVITIES TO PREVENT ADMINISTRATIVE AND STAFF FRAUD....45
7.3.1 INFORMATION TO EMPLOYEES....45
7.3.2 COMMUNICATION STRATEGY....46
7.3.3 SYSTEM CONTROLS....46
7.4 STRATEGIES AND ACTIVITIES TO DETECT ADMINISTRATIVE AND STAFF FRAUD....46
7.4.1 TRANSACTIONAL ANALYSIS....46
7.4.2 IDENTITY ANALYSIS....47
7.4.3 DATA MATCHING....47
7.4.4 SYSTEM CONTROLS....47

7.5 STRATEGIES AND ACTIVITIES TO DETER ADMINISTRATIVE AND STAFF FRAUD 47
7.5.1 MEDIA EXPOSURE 47
7.5.2 PROSECUTIONS 47
7.5.3 PENALTIES 47
8. FRAUD PLAN FOR INFORMATION RISKS 48
8.1 OVERVIEW 48
8.1.1 INFORMATION FRAUD MANAGEMENT FRAMEWORK 49
8.2 KEY RISKS 50
8.3 STRATEGIES AND ACTIVITIES TO PREVENT UNAUTHORISED ACCESS, USE AND DISCLOSURE OF INFORMATION. 50
8.3.1 PRIVACY IMPACT ASSESSMENTS 50
8.3.2 PRIVACY AWARENESS KIT 50
8.3.3 DECLARATION OF CONFIDENTIALITY 51
8.3.4 DENY ACCESS FACILITY 51
8.3.5 CUSTOMER PASSWORDS 51
8.3.6 CLEAR DESK POLICY 52
8.3.7 CHIEF EXECUTIVE INSTRUCTIONS 52
8.3.8 PROCUREMENT PROCESS 52
8.4 STRATEGIES AND ACTIVITIES TO DETECT UNAUTHORISED ACCESS, USE AND DISCLOSURE OF INFORMATION. 52
8.4.1 CUSTOMER RECORD ACCESS MONITOR 53
8.4.2 SECURITY INCIDENTS 53
8.4.3 INVESTIGATION OF SUSPECTED PRIVACY BREACHES 54
8.4.4 PRIVACY COMPLIANCE STRATEGY – BROWSING 54
8.5 STRATEGIES AND ACTIVITIES TO DETER UNAUTHORISED ACCESS, USE AND DISCLOSURE OF INFORMATION. 55
8.5.1 DISCIPLINARY ACTION 55
8.5.2 PROSECUTION AND PENALTIES 55

EXECUTIVE SUMMARY

BACKGROUND:

- The *Commonwealth Fraud Control Guidelines 2002* require that Commonwealth agencies conduct regular fraud risk assessments and produce a Fraud Control Plan immediately following the completion of the risk assessments.
- Centrelink has produced the *Fraud Control Plan 2008-10* to address the specific requirements of the *Commonwealth Fraud Control Guidelines 2002*.

CENTRELINK 2008-10 FRAUD CONTROL PLAN KEY FEATURES:

- Biennial Risk Assessments for Program Fraud, Administrative & Staff Fraud and Information Fraud completed to inform this *Fraud Control Plan*.
- A statement of the agency's attitude and approach to fraud (see the CEO's Introduction, p2).
- Cleary explained links between the *Fraud Control Plan* and Centrelink's Strategic Directions (see section 1.2).
- Details of individual fraud control responsibilities (see section 2).
- Responsibilities that all employees have for fraud control are outlined (see section 2).
- An outline of Centrelink's current organisational structure (see section 4.4).
- Centrelink Fraud Control Framework maps (see sections 6.1.1 for Program Fraud, 7.1.1 for Administrative & Staff Fraud & 8.1.1 for Information Fraud).
- Summary of risks for Program Fraud, Staff & Administrative Fraud and Information Fraud (see sections 6.4, 7.2 & 8.2).
- On going strategies included that address all key risks identified, both internal and external (see sections 6, 7 & 8).
- Links to key performance indicators (see section 6.3).
- Details of relevant awareness raising and training strategies (see sections 5.5, 6.5.6, 6.5.7, 7.3.1, 7.3.2, 8.3.2 & 8.3.3).

1. ABOUT CENTRELINK'S FRAUD CONTROL PLAN

1.1 OVERVIEW

This *Fraud Control Plan* provides internal reference and external assurance of:

- Centrelink's relationship with its policy departments and the payments and services that are delivered on their behalf;
- Centrelink's organisational structure including Centrelink's commitment to and involvement in effective fraud control at each level of the Agency; and
- What Centrelink is, and what it does, to prevent, detect and deter fraud against the:
    - Payments and services it delivers for its policy departments;
    - Information it holds; and
    - Its administrative operations.

It has been compiled to address the specific requirements of the *Commonwealth Fraud Control Guidelines 2002*.

1.2 CENTRELINK'S STRATEGIC DIRECTIONS

The Plan is directly linked to Centrelink's Strategic Directions. The Directions have five core elements that set out Centrelink's reason for being and what Centrelink wants to achieve. The *Fraud Control Plan* is linked to:

- The core value of accountability, which is accepting responsibility for what we do and being transparent in our conduct;
- The importance of governance and its relationship to the roles, accountabilities and capabilities we need to respond to Government and to Centrelink's customers; and
- The strategic theme of demonstrating value for money, which makes us accountable for the efficient and effective use of resources and ensuring the best service offer at the best price.

2. FRAUD CONTROL RESPONSIBILITIES

The following table summarises particular responsibilities of employees and managers. These responsibilities are linked to Centrelink's Strategic Directions (see Chapter 1.2).

Who	Responsibility	Reference
All employees	To familiarise themselves with this *Fraud Control Plan* and to consider fraud control issues in the performance of their duties.	*Fraud Control Plan*.
All employees	To behave ethically and in accordance with guidance on employee behaviour in the performance of their duties.	Section 2 and 7 - *Fraud Control Plan*, the *Public Service Act 1999* and the *APS Values and Code of Conduct.*
All employees	To report suspected incidents of fraud and misconduct.	Section 7 *Fraud Control Plan.*
All employees	To observe directions from the Chief Executive Officer, General Manager—People and Ministerial, and Business Manager—Internal Assurance Section, in the conduct of enquiries related to suspected fraud and misconduct.	Section 7 and 8 *Fraud Control Plan* and *Declaration of Confidentiality*.
All employees	Knowledge of and compliance with IT Security Policy, Electronic Facilities Guidelines and APS Values & Code of Conduct.	Sections 2, 7 and 8 *Fraud Control Plan*, Centrelink Security Policy, e-Mail and Internet Code of Conduct
All employees	Knowledge of and compliance with financial delegations, including spending approvals.	Section 7 *Fraud Control Plan,* Centrelink Spending Approver Tool and Spending Delegation User Guide.
Credit Card Holders	Knowledge of and compliance with Centrelink's financial delegations, credit card policy and spending approvals.	Section 7 *Fraud Control Plan,* Centrelink Spending Approver Tool and Spending Delegation User Guide.
Cabcharge Card holders	Knowledge of and compliance with Centrelink's financial delegations, Cabcharge policy and spending approvals.	Section 7 *Fraud Control Plan*, Centrelink Spending Approver Tool and Spending Delegation User Guide.
All Centrelink employees and contractors who have access to a fuel card	Knowledge of and compliance with Centrelink's financial delegations and spending approvals.	Section 7 *Fraud Control Plan*, Centrelink Spending Approver Tool and Spending Delegation User Guide.
Deputy Chief Executive Officer - Clients, Capability & Corporate	Ensure the integrity of outlays.	Section 2, 4, 5, 6, 7 and 8 *Fraud Control Plan*
General Manager, People & Ministerial Division	People capability & strategic planning.	Section 2, 4, 5, 7 & 8 *Fraud Control Plan*
National Manager, People Development and Training Branch	Education and Training.	Sections 4, 5 and 6 *Fraud Control Plan*
National Manager, People	Leadership in Centrelink. Code of	Section 2, 7 & 8 *Fraud*

Who	Responsibility	Reference
Strategy Branch	Conduct sanctions.	*Control Plan*
National Manager, People Services Branch	Code of Conduct policy.	Section 7 & 8 *Fraud Control Plan*
General Manager, Client Business Division	Develop BPA commitments with client departments.	Section 6 *Fraud Control Plan*
Chief Financial Officer Finance Division	Lead and support financial and business capability to satisfy government expectations and Centrelink's corporate strategy and accountability. Assure CEO of Centrelink compliance with Fraud Control Guidelines. Co-ordinate production of the Fraud Control Plan.	Sections 2, 4, 5, 6, 7 and 8 *Fraud Control Plan*
National Manager, Legal Services & Procurement Branch	Develop policy guidelines and procedures and investigates alleged breaches of privacy and confidentiality. Provide legal advice on privacy, confidentiality and fraud. Ensure there are appropriate policies and controls in place in all areas of contract management and procurement.	Sections 2,4, 6, 7 and 8 *Fraud Control Plan*
National Manager, Financial Management and Services Branch	Develop policies, procedures and systems to help control financial risk.	Sections 4, 5 and 7 *Fraud Control Plan*
General Manager, Communication Division	Increase awareness of fraud issues.	Sections 6, 7 of *Fraud Control Plan*
Deputy Chief Executive Officer - Information Technology	Ensure that effective IT strategies are in place.	Section 2, 4, 5 and 8 *Fraud Control Plan*
General Manager, Corporate IT Systems Division	Provide a security and information protection service.	Sections 2, 4, 5 and 8 *Fraud Control Plan*
National Manager, Security and Information Protection Branch	Provide and implement strategies for the protection of Centrelink assets and information and provide security for assets and employees.	Sections 2, 4, 5 and 8 *Fraud Control Plan*
Deputy Chief Executive Officer - Customer Service	Successfully deliver the Government's employment and social security policy.	Section 2, 4, 5 and 6 *Fraud Control Plan*
General Manager, Education, Employment & Support Programs Division	Undertake program risk assessments (including fraud risks).	Sections 4, 5 and 6 *Fraud Control Plan*
General Manager, Families, Seniors & Business Integrity Division	Undertake program risk assessments (including fraud risks), prepare Annual Business Assurance Statements to policy departments and develop appropriate Payment Integrity Action Plans. Manage performance expectations and ensure that an effective quality agenda is in place to assure processes. Manage debt, compliance, fraud and assurance issues.	Sections 2, 4, 5 and 6 *Fraud Control Plan*

Who	Responsibility	Reference
National Manager, BI Programs Branch	Research, analyse and develop strategies for improving overall levels of compliance and reducing fraud. Oversee the conduct of payment integrity risk assessments and analysis in relation to Centrelink's major programs. Develop an end-to-end compliance and review model for the selection, delivery and reporting of review activities; delivery of review initiatives developed through Budget or internal processes and manage the compliance media strategy.	Sections 4, 5 and 6 *Fraud Control Plan*
National Manager, BI Operations Branch	Develop and implement strategies for the prevention, detection, and deterrence of fraud and recovery of debt.	Sections 2, 4, 5 and 6 *Fraud Control Plan*
National Manager, BI Performance Branch	Provide statistical reports against the allocation of process related funding to Areas that provide a prescribed range of services through a defined range of business processes, practices and structures.	Section 5 and 6 of *Fraud Control Plan*
General Manager, Audit, Governance & Assurance Division	Responsible for being alert to instances of internal fraud during internal audit assignments and passing details of possible or actual instances of fraud to the Business Integrity Network or Internal Assurance Section, as appropriate and as rapidly as possible. Provide strategies and processes for preventing, deterring, detecting and investigating internal fraud.	Section 2, 4 and 7 *Fraud Control Plan*
Internal Assurance Section	Detection and deterrence of employee fraud. Prepare Employee Fraud and Conduct Control Action Plan.	Sections 2 and 7 *Fraud Control Plan*
Audit Committee	Review Centrelink's *Fraud Control Plan* and satisfy itself that Centrelink has appropriate processes and systems in place to capture and effectively investigate fraud related information. Assist the CEO with responsibilities for financial reporting, maintaining an efficient system of internal controls, improving performance and accountability and reviewing specific matters that may arise from the external audit process.	Section 4 *Fraud Control Plan*

2.1 WHAT ARE CENTRELINK'S STANDARDS FOR EMPLOYEES AS THEY RELATE TO THE FRAUD CONTROL PLAN?

2.1.1 INTEGRATED LEADERSHIP SYSTEM (ILS)

The Integrated Leadership System provides capability development guidance for individuals and agencies in the form of descriptions and behaviours for all levels in the APS. In relation to the *Fraud Control Plan*, this means leading by example and producing a plan that provides clear guidance about what is expected in relation to fraud control.

2.1.2 AUSTRALIAN PUBLIC SERVICE CODE OF CONDUCT AND VALUES

All Centrelink employees are bound by the *Public Service Act 1999* (the Act) which requires that employees behave in a manner that upholds the Australian Public Service (APS) Values and complies with the APS Code of Conduct. The APS Values are set out in Section 10 of the Act. The APS Code of Conduct is set out in section 13 of the Act.

The APS Code of Conduct requires, among other things, that an employee:

- Behave honestly and with integrity in the course of employment;
- Act with care and diligence in the course of employment;
- Treat everyone with respect and courtesy, and without harassment; and
- Comply with all applicable Australian laws.

Disciplinary action may be taken if employees fail to comply with the required standards.

2.1.3 INFORMATION TO EMPLOYEES

Centrelink employees play an important role in the prevention of fraud. Ensuring that employees have access to guidelines and protocols that are accurate and easily accessible is vital to having effective fraud prevention strategies in place.

Centrelink takes a pro-active approach towards training and keeping employees informed. This includes providing ongoing information to employees about the:

- Methods for prevention, detection and deterrence of fraud;
- Risk of detection of employee fraud; and
- Penalties that apply to employees engaged in internal fraud.

Centrelink provides the following publications, reference material and training packages to keep employee's informed about fraud on a regular basis:

- The *Fraud Control Plan*;
- The National Induction Program;
- The Centrelink Administrative Reference Suite;
- The Internal Fraud Awareness Kit;

- The External Fraud Awareness Kit;
- The Centrelink Security Policy Manual;
- The Privacy Awareness Kit;
- Declaration of Confidentiality; and
- Getting it Right.

This reference material is available on Centrenet.

Centrelink also provides information on fraud through internal channels such as:

- Screen Savers;
- Centrelink Update;
- CEO's Message;
- Frontline Manager;
- Network and NSO newsletters;
- *Centrelink People;* and
- Business Television.

2.1.4 CHIEF EXECUTIVE INSTRUCTIONS

Section 44 of the Financial Management & Accountability Act requires a Chief Executive Officer (CEO) of an agency to manage the affairs of the agency in a way that promotes the efficient, effective and ethical use of Commonwealth resources – which includes compliance with applicable laws and Australian Government policy.

Chief Executive Instructions (CEI) issued under section 52 of the FMA Act are a means of ensuring compliance with section 44 of the FMA Act. CEI's are an important governance mechanism by which the CEO prescribes Centrelink's policies and procedures.

Centrelink CEI's cover a wide range of subjects and include directions relating to:

- Protective Security (CEI 2);
- Management and Control of Public Property (CEI 10);
- Procurement of Property (Goods) and Services (CEI 12);
- Financial Policy Instructions and Financial Procedures (CEI 4);
- Expenditure of Public Money (CEI 8);
- Unauthorised Access to Centrelink Customer Records and the Personnel Records of Centrelink Employees (CEI 20);
- Centrelink Employees Interacting with Centrelink as Customers (CEI 21);
- Records Management (CEI 17); and
- Management and Control of Public Money (CEI 7).

2.2 HOW DOES CENTRELINK PROTECT ITS EMPLOYEE AND CUSTOMER INFORMATION?

Centrelink has developed a protective security framework to ensure that the delivery of Centrelink's payments and services is protected from current and emerging threats, consistent with risk management principles and standards of the Australian Government and Centrelink.

The protective security framework covers the protection of information and the provision of a secure environment for employees and for Centrelink's customers. Centrelink's physical, personnel and information security is consistent with the policy requirements of the Australian Government, as set out in the *Protective Security Manual 2005* *(as amended 2007*) and the Australian Government Information and Communications Technology Security Manual (ACSI33). Centrelink security policy and standards are set out in the Centrelink Security Policy Manual. The protective security framework provides the high level controls within which privacy and fraud management controls are developed.

Security risk reviews and assessments are conducted against business and services to mitigate risk and to achieve compliance with security policy, procedures and standards. To enhance security protection of its information holdings and to ensure a safe business environment for employees and for Centrelink's customers, Centrelink has implemented the following measures:

- Conduct security reviews of protective security across Centrelink;
- Development and review of site security plans for over 400 Centrelink sites;
- Conduct of security reviews of security incidents at Customer Service Centres;
- Reviews of specific sites;
- Conduct of security risk assessments of Centrelink;
- Development and review of the Agency Security Plan; and
- Development of security training and awareness programs.

As the risk mitigation strategies are identified, they are documented in Centrelink's Agency Security Plan and Information & Communications Technology (ICT) system security assessments and system security plans.

See also Section 8 – Information Risks.

2.2.1 PHYSICAL SECURITY

Physical security within Centrelink is designed to prevent unauthorised access to Centrelink premises and to detect and respond to intruders. Employees are required to follow minimum security standards.

2.2.2 PERSONNEL SECURITY

All Centrelink employees and contractors undergo police checks. Employees and contractors requiring access to information security classified at levels above IN-CONFIDENCE undergo an appropriate security clearance.

2.2.3 INFORMATION AND COMMUNICATIONS TECHNOLOGY SECURITY

Information and Communications Technology (ICT) security within Centrelink is designed to prevent the unauthorised access to, and disclosure of, official information.

Centrelink provides access to its information resources for three main user groups, i.e. employees, Centrelink business partners and Centrelink customers.

Employee access is controlled by 2-factor authentication (Accesslink, being replaced in 2009 by the Centrelink Staff Identification Card [smartcard]). Employee access to resources within Centrelink is controlled by Security Access Management System (SAMS).

Access and authentication services for customer on-line services is controlled by technical controls set out in the Self-service Access and Authentication Policy. This framework is based on the principle that electronic transactions or services are only made available to user groups where the relative risk of unauthorised access or misuse of resources has been reduced to an acceptable level. The security requirements of all electronic services are assessed against this framework and the access and authentication controls applied in accordance with the risk outcome.

To manage technical security risk, Centrelink:

- Maintains an external gateway, annually certified to Defence Security Directorate (DSD) standards;
- Communication to business partners via FedLink for subscribing Australian Government agencies and dedicated encrypted links to other organisations;
- Issues encrypted laptops and maintains a Virtual Private Network (VPN) to permit secure communication between employees and Centrelink for off-site work;
- Provides customers with Secure Online Mail (SOM) and Secure Internet Messaging Service (SIMS) for secure electronic communication with Centrelink;
- Maintains and enhances its anti-malware capabilities to prevent compromise of its servers and desktops from viruses and other malicious code originating from Internet based web and email services;
- Monitors IT equipment configuration to protect and detect equipment compromise; and
- Implements (in 2008) end-point security to encrypt and manage removable media, including USB drives level.

3. WHAT IS FRAUD CONTROL?

3.1 DEFINITION OF FRAUD

The *Commonwealth Fraud Control Guidelines 2002*, define fraud against the Australian Government as:

Dishonestly obtaining a benefit by deception or other means.

This definition includes:

- Theft;
- Obtaining property, a financial advantage or any other benefit by deception;
- Causing loss, or avoiding or creating liability by deception;
- Providing false or misleading information to the Australian Government, or failing to provide information where there is an obligation to do so;
- Making, using or processing forged or falsified documents;
- Bribery, corruption or abuse of office;
- Unlawful use of Australian Government computers, vehicles, telephones and other property or services;
- Relevant bankruptcy offences; and
- Any offence of a like nature to those listed above.

3.2 FRAUD IN CENTRELINK

Centrelink has categorised and defined the following types of fraud:

- **Payment Fraud**–can involve customers and non-customers. It includes providing false information to claim payment; failure to declare circumstances fully; deliberate failure to notify a change of circumstance; or providing false advice of changed circumstances according to the relevant legislation.
- **Staff Fraud**–is the misappropriation by employees of program funds and services administered by Centrelink. Misappropriation may be either for personal gain or to deliberately overpay another person.
- **Administrative Fraud**–occurs when either Centrelink employees or persons outside of Centrelink use resources for purposes other than for which they were provided. This can involve stealing property for personal use, manipulating salaries or fraudulently claiming overtime. It may also involve people outside Centrelink attempting to fraudulently obtain Centrelink's administrative resources.
- **Information Fraud**–is the theft or misuse of information held by Centrelink. It occurs when employees make inappropriate use of information they have access to as part of their duties. The benefit obtained may be tangible or intangible. An example of a tangible benefit would be the selling or provision of customer details to third parties (e.g.

private investigators). An intangible benefit may be obtaining personal information about a colleague, or others, which you are not entitled to access. Information fraud can also include unauthorised access to Centrelink's computer systems from people outside the organisation (hackers).

3.3 FRAUD CONTROL IN CENTRELINK

Fraud Control in Centrelink is based on the following principles:

- Prevention of fraud;
- Detection and investigation of fraud;
- Deterrence of fraud through:
    1. Prosecution of offenders, including in minor instances of fraud where appropriate;
    2. Application of appropriate civil, administrative or disciplinary penalties; and
    3. Recovery of proceeds of fraudulent activity;
- Training of all employees to provide them with an awareness of ethics, privacy and fraud;
- Specialised training of employees involved in fraud control activities; and
- Reporting to Government and accountability to Parliament.

4. ABOUT CENTRELINK

4.1 OVERVIEW

Centrelink is a statutory agency within the Department of Human Services Portfolio.

Centrelink delivers a range of Australian Government services to 6.5 million customers. Centrelink customers include retirees, families, sole parents, people looking for work, people with a short-term incapacity, people with disabilities, carers, students, young people, Indigenous people and people from diverse cultural and linguistic backgrounds.

Centrelink was established by the *Commonwealth Services Delivery Agency Act 1997* (CSDA Act) as an agency under the *Financial Management and Accountability Act 1997* (FMA Act). It is staffed under the *Public Service Act 1999*.

4.2 NATIONAL SUPPORT OFFICE

The National Support Office is Centrelink's headquarters and is located mainly in Canberra with some teams outposted to other locations. It supports the Minister, policy departments, Area Support Offices and the Centrelink Network.

4.2.1 THE CHIEF EXECUTIVE OFFICER

The Chief Executive Officer is responsible for the day-to-day administration and control of Centrelink's operations. His functions and accountabilities include entering into service arrangements with the heads of policy departments, implementing strategies, measuring financial and operational performance, and reporting to the Minister for Human Services.

In order to meet his accountabilities the Chief Executive Officer delegates responsibilities to those senior executives who report directly to him, and holds them accountable for their decisions and actions taken on his behalf. Together with the Chief Executive Officer, this group forms the Centrelink Executive.

The Centrelink Executive consists of:

- The Chief Executive Officer;
- The Deputy Chief Executive Officer Clients, Capability and Corporate;
- The Deputy Chief Executive Officer Customer Service; and
- The Deputy Chief Executive Officer Information Technology.

The Chief Executive Officer is also assisted by a number of strategic committees (refer to Section 4.5). Strategic Committees have been established where:

- A joint commitment is required (contributing decisions are required by accountable people from different groups);
- The decision being taken has significant impact on cross Agency/Group/Division stakeholders; or

- It is important to have a clear record of decisions and accountability for a complex or cross program matter.

Within the National Support Office framework, there are specialist groups that have the management responsibility for preventing, detecting, deterring and investigating cases or instances of fraud. An overview of these specialist groups follows.

4.2.2 CHIEF FINANCIAL OFFICER- FINANCE DIVISION

The Finance Division's role is to lead and support financial and business capability to satisfy government expectations and Centrelink's corporate strategy, accountability and legal obligations. It has responsibility to understand the financial environment in which Centrelink operates and develops policies, procedures and systems to help control financial risk.

The Chief Financial Officer is responsible for:

- Coordination, production and approval by the CEO and the Audit Committee of the *Fraud Control Plan* every two years; and
- Producing an agency fraud health check based on ANAO recommended checklist to provide assurance to the CEO that Centrelink is meeting its obligations under the Fraud Control Guidelines.

The Finance Division, through the Privacy & Information Access Section, is responsible for investigating alleged breaches of privacy and confidentiality.

4.2.3 CORPORATE IT SYSTEMS DIVISION

The Corporate IT Systems Division supports Centrelink's Purpose and Strategic Directions by providing modern, reliable, secure and current IT infrastructure, production IT services and corporate systems. They ensure that:

- Centrelink has a modern, reliable and secure platform for IT systems; and
- IT systems and services operate reliably, efficiently and effectively.

The Corporate IT Systems Division is responsible for the following outputs:

- Developing and maintaining reliable, efficient and effective infrastructure and corporate IT systems;
- Providing effective information protection services;
- Managing IT services which meet the requirements of Service Level Agreements; and
- Ensuring Centrelink has a rigorous project management and coordination capability.

4.2.4 FAMILIES, SENIORS AND BUSINESS INTEGRITY DIVISION

The Families, Seniors and Business Integrity Division is responsible for ensuring the integrity of Centrelink outlays and services by minimising fraud and customer debt.

To do this it develops and implements strategies for the prevention, detection, and deterrence of fraud and recovery of debt.

The Division is also responsible for developing an end-to-end compliance and review model for the selection, delivery and reporting of review activities. It also delivers review initiatives developed through Budget or internal processes and manages Centrelink's compliance media strategy.

The Division undertakes research, analyses and develops strategies for improving (and measuring the improvement in) business integrity outcomes, including levels of compliance, fraud and non-payment outcomes. It also oversees the conduct of payment integrity risk assessments in relation to Centrelink's major programs, in collaboration with other parties including policy departments.

The Business Integrity Network is responsible for prescribing business processes, practices and structures required to deliver business integrity services. They are also responsible for providing the BI Performance Branch with comprehensive performance data and analysis.

4.2.5 PEOPLE AND MINISTERIAL DIVISION

The People and Ministerial Division is responsible for the provision of human resource advice and policy, and related administration for Centrelink on a national basis. This also includes, but is not limited to, business ownership of the Infolink HR system, Ethics policy, Code of Conduct policy and any subsequent action involved in resulting disciplinary processes. It ensures Centrelink has a skilled workforce able to deliver on agreed business commitments, aligned with Centrelink's strategic directions.

4.2.6 AUDIT, GOVERNANCE AND ASSURANCE DIVISION

The role of the Audit, Governance and Assurance Division is to provide independent assurance on the performance of management in maintaining Centrelink's strategic direction, achieving its operational objectives in line with organisational and legislative requirements, and ensuring that the highest standards of probity and accountability are met. In doing so, the Audit, Governance and Assurance Division forms part of the organisation's governance framework – providing an integral contribution to governance, risk management and control within Centrelink.

It is also responsible for investigating incidents of internal fraud.

4.2.6.1 Audit Committee

The Audit Committee is a standing committee which has the broad objectives of:

- Assisting the CEO to ensure Centrelink meets its strategic objectives;
- Promoting accountability to the Minister, the Parliament, Policy Departments and the community;
- Supporting measures to improve management performance and internal controls;

- Overseeing the Internal Audit function; and
- Ensuring effective liaison between senior management, Centrelink Audit and external audit.

The Audit Committee is not a sub-committee of the Centrelink Executive, and differs from the other Strategic Committees in that:

- It is chaired by an external, independent chair;
- Its members may vote on decisions before the Committee; and
- It supports the CEO directly.

The Audit Committee's functions include monitoring risk exposures in fraud control and security reports and other risk management strategies and reports.

4.3 CUSTOMER SERVICE DELIVERY

4.3.1 AREA NETWORK

Centrelink has grouped its Customer Service Centres and support services into 15 geographical Areas around Australia, each with an Area Support Office, headed by an Area Manager. The Area Support Offices provide management, administrative and operational support for the Customer Service Centres and specialist services within each area.

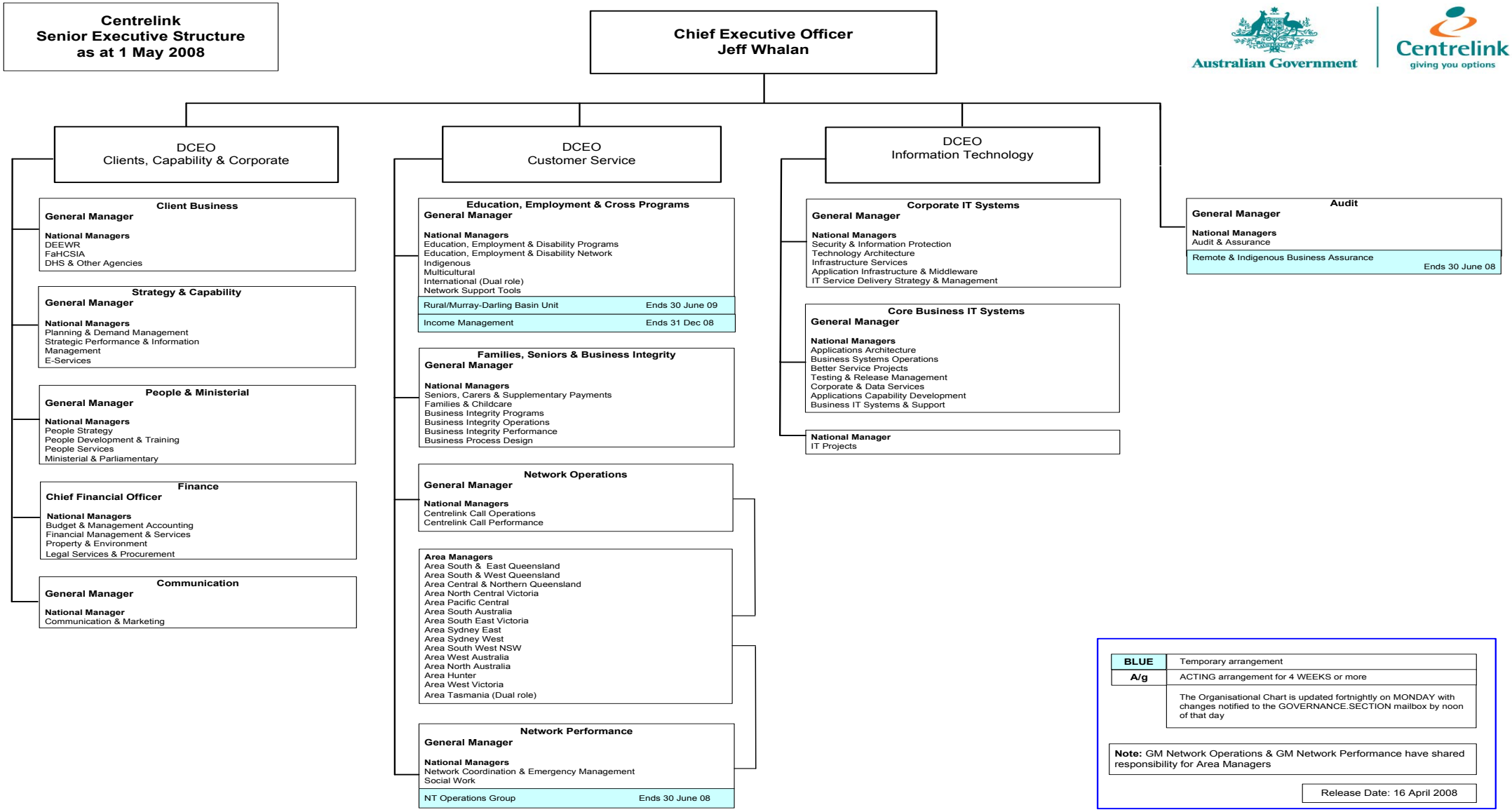
4.3.2 CUSTOMER SERVICE NETWORK

Centrelink's Customer Service Network includes Customer Service Centres and Call Centres, along with other specialist customer service outlets and community agents. The network provides services funded by Centrelink's policy departments directly to customers. There are 704 Customer Service Centres, Centrelink agents, Indigenous community agents, Remote Area Service Centres and 25 Call Centres.

4.3.3 CUSTOMER SERVICE SUPPORT CENTRES

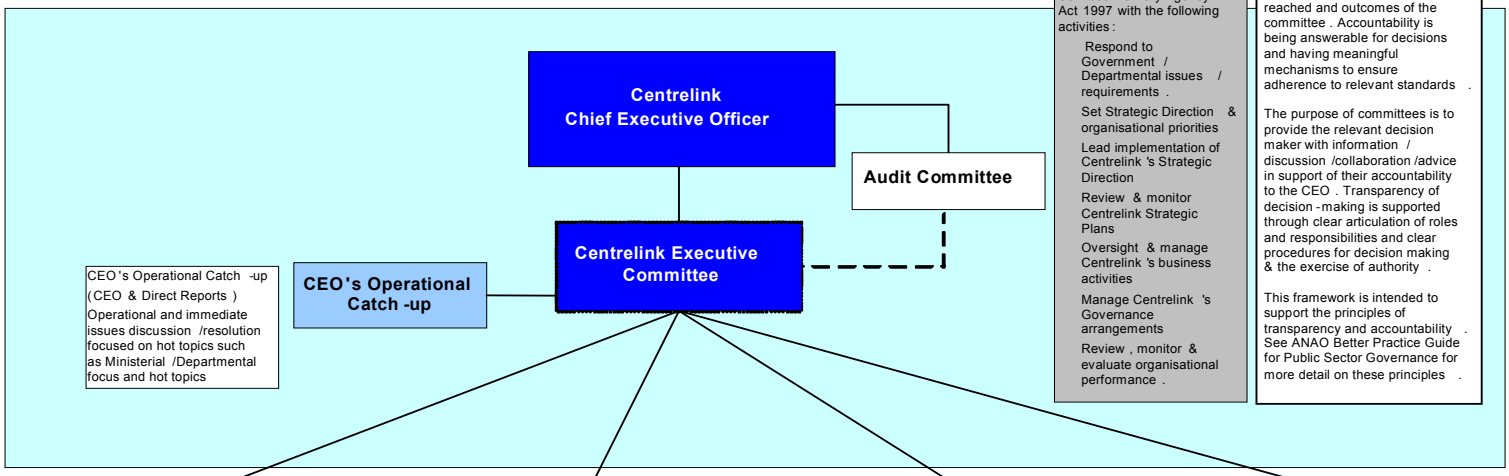
Customer Service Support Centres (CSSCs) consolidate appropriate activities nationally to maximise customer access, quality service and efficiency.

4.4 CENTRELINK ORGANISATIONAL STRUCTURE & STRATEGIC COMMITTEE FRAMEWORK



Australian Government | Centrelink giving you options

Strategic Committee Framework



Centrelink Executive Committee

The Centrelink Executive Committee meets monthly to support the CEO in meeting his responsibilities in line with the Commonwealth Services Delivery Agency Act 1997 with the following activities:

- Respond to Government / Departmental issues / requirements .
- Set Strategic Direction & organisational priorities
- Lead implementation of Centrelink 's Strategic Direction
- Review & monitor Centrelink Strategic Plans
- Oversight & manage Centrelink 's business activities
- Manage Centrelink 's Governance arrangements
- Review , monitor & evaluate organisational performance .

Centrelink Committee Governance Principles

Accountability rests with the incumbent of individual positions , in the committee context the Chair of each committee is accountable for the decisions reached and outcomes of the committee . Accountability is being answerable for decisions and having meaningful mechanisms to ensure adherence to relevant standards .

The purpose of committees is to provide the relevant decision maker with information / discussion /collaboration /advice in support of their accountability to the CEO . Transparency of decision -making is supported through clear articulation of roles and responsibilities and clear procedures for decision making & the exercise of authority .

This framework is intended to support the principles of transparency and accountability . See ANAO Better Practice Guide for Public Sector Governance for more detail on these principles .

Strategy , Planning & Resources Committee (CEO)

PURPOSE

To set and progress the strategic direction of Centrelink .

ACTIVITIES

Set the medium to long -term strategy for Centrelink .

Agree short -term strategies to support Centrelink 's long -term strategy .

Consider the relationship between current strategies and Centrelink 's future capability requirements .

Determine plans to position Centrelink for providing excellence in service delivery .

Promote and support the alignment of Centrelink 's strategies and plans with resourcing requirements .

Evaluate the impacts of the strategies and plans and their implementation , across Centrelink .

Allocate resources within Centrelink - including capital and project investment and budget allocations .

Monitor the implementation of strategies and plans , including the allocation of resources .

Report to the Centrelink Executive Committee .

People Committee (DCEO SR)

PURPOSE

To set the strategic direction for Centrelink 's people capability .

ACTIVITIES

Prioritises workforce issues and initiatives to ensure Centrelink has a skilled workforce able to deliver on Government initiatives and agreed business commitments aligned with the Strategic People Plan .

Oversees Centrelink 's workplace relations framework in support of the achievement of the Strategic People Plan .

Sets Centrelink 's learning strategy and monitors Centrelink 's strategic priority to attract , train and retain skilled people to deliver customer outcomes .

Provides leadership and advice to branches /divisions /group and other strategic committees on matters relating to people to ensure the successful implementation of Centrelink 's Strategic People Plan and governance framework .

Provides strategic advice to the Strategy , Planning and Resources Committee and to the Centrelink Executive Committee on all matters relating to Centrelink people that impact on Centrelink 's ability to deliver the services required by Government .

Oversees that Centrelink 's people policies and initiatives meet legal and legislative requirements and that they are consistent with the Strategic People Plan in terms of context and priority .

Supports the alignment of financial , people and IT resources to the Centrelink Strategic Business Plan , and provides assurance to the Centrelink Executive Committee that Centrelink resources are being managed appropriately and can be delivered effectively through risk identification and mitigation .

Reports to the Centrelink Executive Committee .

IT Committee (DCEO IT)

PURPOSE

To assist the Centrelink Executive Committee in governing & overseeing Centrelink 's IT related matters & ensuring that Centrelink has effective IT Governance frameworks in place .

A forum for the DCEO IT to discuss strategic IT decisions on IT direction & operation in the context of the Centrelink Strategic Directions .

ACTIVITIES

Monitors business alignment processes are in place to build confidence in Centrelink 's IT - that is , IT supports the Centrelink Strategic Directions and that business leverages future technology trends and opportunities .

Monitors policies , processes and frameworks are in place for effective management of IT in Centrelink .

Provides IT strategic direction by :

- Reviewing & approving the IT Group Plan and Divisional Plans .
- Reviewing & approving architectural directions .

Monitors delivery against the IT Group Plan and Divisional Plans .

Prioritises and approves IT Projects to meet Architectural solutions .

Monitors IT project delivery , including Refresh .

Provides assurance to the organisation that IT is being managed appropriately and can deliver effectively by :

- Monitoring IT risk identification & mitigation .
- Monitoring IT capability management including sourcing arrangements .
- Monitoring IT service performance and productivity & assessing IT contribution to Centrelink .

Reports to the Centrelink Executive Committee .

Performance Committee (DCEO CS)

PURPOSE

The Performance Committee assures the Chief Executive Officer that Centrelink 's performance meets the Government and Policy Department requirements .

ACTIVITIES

Monitors performance to ensure that , through the Statement of Intent , we achieve the Minister 's Statement of Expectations .

Reports on :

- Achievement of Key Performance Indicators (KPIs) in Business Partnership Agreements (BPA) and other business agreements .
- Initiates corrective action where required .
- the alignment and appropriateness of performance measures to Centrelink 's overall organisational risks .
- the impact of change and future demand across all channels in relation to performance .
- Informs the development of strategies and plans through interactions with the Strategy , Planning and Resources Committee .

Reports to the Centrelink Executive Committee .

Release Date & Version (26 June 2007 - 04/2007)

5. WHAT DO THE COMMONWEALTH FRAUD CONTROL GUIDELINES MEAN FOR CENTRELINK?

5.1 OVERVIEW

The *Commonwealth Fraud Control Guidelines 2002* outline the Government's requirement that Australian Government agencies put in place a comprehensive fraud control program that includes prevention, detection, investigation and reporting strategies.

Agencies should consider prosecution in appropriate circumstances, in accordance with the *Prosecution Policy of the Commonwealth*. Criminal prosecutions are vital to deterring future instances of fraud and to educating the public generally about the seriousness of fraud.

Agencies should also be committed to recovering losses caused by illegal activity through proceeds of crime and civil recovery processes and, in the absence of criminal prosecution, to applying appropriate civil, administrative or disciplinary penalties.

The *Commonwealth Fraud Control Guidelines 2002* apply to:

- All agencies covered by the *Financial Management and Accountability Act 1997; and*
- Bodies covered by the *Commonwealth Authorities and Companies Act 1997* that receive Commonwealth Government funding or funding from Australian Government agencies for at least 50 per cent of their operating costs.

The Chief Executive Officer (CEO) has principal responsibility for fraud control within Centrelink and for complying with the *Commonwealth Fraud Control Guidelines 2002.* In order to comply with the guidelines Centrelink needs to:

- Develop an overall fraud control strategy for the agency, including operational arrangements for dealing with fraud;
- Conduct fraud risk assessments;
- Produce a *Fraud Control Plan*;
- Investigate instances of fraud against Centrelink including minor instances;
- Train employee's involved in fraud control to specified levels of competency;
- Report on fraud control activities;
- Foster and maintain the highest standards of ethical behaviour to comply with the Guidelines on Official Conduct for Commonwealth Public Servants and the Public Service Act 1999 - APS Values and APS Code of Conduct;
- Inform the Minister of all relevant fraud control initiatives undertaken; and

- Certify in the Annual Report that:
    - Fraud risk assessments and fraud control plans have been prepared that comply with the Commonwealth Fraud Control Guidelines;
    - Appropriate fraud prevention, detection, investigation and reporting procedures and processes are in place; and
    - Annual fraud data has been collected and reported that complies with the Commonwealth Fraud Control Guidelines.

These responsibilities continue, even when Centrelink contracts part of its service delivery or fraud control activities to external service providers.

In line with CEOs' responsibilities for developing an overall fraud control strategy, Centrelink is also required to prepare and widely distribute within Centrelink a statement of Centrelink's approach and policy towards fraud.

5.2 REPORTING

The *Commonwealth Fraud Control Guidelines 2002* require that extensive management information relating to fraud be provided to the Attorney-General's Department in order for it to produce the Annual Report on Fraud Control.

The categories of information required from each agency covered by the *Commonwealth Fraud Control Guidelines 2002* include:

- Case flow and incident information;
- Losses;
- Offenders;
- Agency fraud resources;
- Training; and
- Prevention and detection activity.

Centrelink collects Management Information on fraud related activities via a number of electronic systems, including:

- The Fraud Investigation and Case Management System;
- The Debt Management System;
- The Privacy and Investigation Reporting System; and
- The Integrated Review System.

The responsibility for gathering and reporting the required information to the Attorney Generals Department rests with National Manager, Business Integrity Operations.

5.2.1 OTHER REPORTING

Centrelink provides the Australian Federal Police with an annual list of major fraud risks together with copies of current fraud risk assessments. Centrelink also provides six monthly reports to policy departments on identity fraud review activity.

Centrelink's Executive is provided with a monthly report that provides a summary of national Business Partnership Agreement compliance (by policy department), internal compliance and fraud activity. The Audit Committee is also provided with a quarterly report on Prosecutions and Identity Fraud.

5.3 RESPONSIBILITIES

5.3.1 THE COMMONWEALTH DIRECTOR OF PUBLIC PROSECUTIONS

The Commonwealth Director of Public Prosecutions (CDPP) is responsible for prosecuting offences against Commonwealth law and for conducting related criminal assets recovery. All prosecutions and related decisions are made as set out in the *Prosecution Policy of the Commonwealth.*

As stated in the *Commonwealth Fraud Control Guidelines 2002*, instances of fraud are to be investigated and where appropriate prosecuted in accordance with the requirements of the *Prosecution Policy of the Commonwealth*. Centrelink's role in the prosecution process is to investigate cases where it appears that an offence has been committed and to forward such cases to the CDPP for a decision on whether prosecution should proceed, or to refer more complex matters for investigation by the Australian Federal Police.

5.3.2 THE ATTORNEY-GENERAL'S DEPARTMENT

The Attorney-General's Department provides advice to the Minister for Justice and Customs on fraud control issues. Centrelink contributes to the Attorney-General's Department's Annual Report on fraud against the Australian Government in line with the *Commonwealth Fraud Control Guidelines 2002*.

5.3.3 THE AUSTRALIAN FEDERAL POLICE

The Australian Federal Police (AFP) is responsible for investigating serious or complex crime against Commonwealth interests. As Centrelink is responsible for investigating its own instances of suspected fraud, the specialised services of the AFP can be a valuable resource during an investigation. Centrelink can seek guidance as to when a case should be referred to the AFP and the likelihood of the case being accepted under their *Case Categorisation and Prioritisation Model*.

Under the *Commonwealth Fraud Control Guidelines 2002*, Centrelink is exempt from referring all instances of potential serious or complex fraud offences to the AFP. The exemption has been given as Centrelink has the capacity and the appropriate skills and resources needed to investigate criminal matters and meets the requirements of the CDPP in gathering evidence and preparing briefs of evidence.

Once Centrelink has referred a fraud case to the AFP, and the case is accepted for investigation under the *Case Categorisation and Prioritisation Model*, Centrelink is kept informed of the progress of the investigation through the Quarterly Case Management Reports.

Centrelink is required to advise the AFP annually of its current identified major fraud risks to assist them in the provision of appropriate investigative services to agencies.

5.3.3.1 Service Level Agreement with the Australian Federal Police

This agreement facilitates a cooperative partnership between Centrelink and the AFP. It provides a platform for the development of innovative approaches to fraud control in relation to the payments administered by Centrelink. This includes an enhanced focus on intelligence driven fraud detection, a capacity for joint operations and enhanced training opportunities.

5.4 FRAUD CONTROL PLANNING

The scale and geographical spread of Centrelink's operations and the nature of our business makes it impossible to detect and eliminate all fraud, however it is essential that resources are deployed in the most cost effective manner to attain three objectives:

- **Prevention**–to have systems and procedures in place that minimise the risk of fraud;
- **Detection**–to detect fraud at the earliest possible stage if it does occur; and
- **Deterrence**–to deal decisively with the cases that are detected, thus creating recognition of the risks and penalties involved in attempting to defraud Centrelink and to promote voluntary compliance.

This *Fraud Control Plan* is an overarching view of fraud control strategies within Centrelink. It is supported by *Fraud Control Action Plans*. These *Fraud Control Action Plans* specifically address various types of fraud within Centrelink and detail the controls for the individual risks and the strategies and priorities for the period. The action plans are the responsibility of the program areas. The plans are for internal use only.

The *Fraud Control Plan* has been informed by a series of Fraud Risk Assessment Workshops. Workshops were conducted for Centrelink's client departments against the payments that Centrelink delivers. Administrative, staff and information fraud risks have been assessed.

Fraud risk assessments are the responsibility of the program business owners. It is a requirement that these are undertaken every two years. The business owners will need to report the findings of the risk assessment to the Business Integrity Strategic Committee and the Audit Committee.

5.5 FRAUD CONTROL TRAINING

The *Commonwealth Fraud Control Guidelines 2002* set the following mandatory training requirements:

- All Commonwealth employees primarily engaged in the investigation of fraud attain the Certificate IV in Government (Investigation); and
- All Commonwealth employees primarily engaged in the coordination and management of fraud control investigations attain the Diploma of Government (Investigation).

These standards are an ongoing requirement for employees commencing duties in Centrelink fraud teams to attain within 12 months.

Training material is developed to meet the specific requirements of Centrelink as well as overall Australian Government standards. External training providers may be used to either guide employee's through the Certificate IV in Government (Investigation) Recognition of Current Competency process and/or provide training. Where Centrelink uses an external training provider, they must use the materials developed by Centrelink, as a Registered Training Organisation, to ensure that the training is relevant to the job functions.

External training providers are also used to train employees in the Diploma of Government (Investigation), as well as provide other specialist courses for Centrelink fraud employees.

Centrelink undertakes regular assurance reviews of the contracted training providers to ensure that they provide a quality service with:

- Technical expertise in regards to training delivery;
- Material that is relevant; and
- Assessments that continue to adhere to the Australian Quality Training Framework (AQTF).

Internal learning assurance will focus on the Business Integrity Network People conducting comprehensive skills analysis of the employee learning profile and People and Ministerial Division, People Development and Training Branch ensuring that assessment of competencies are completed with integrity.

5.6 RISK MANAGEMENT

Centrelink has adopted a comprehensive organisation wide corporate risk management framework. The key objectives of this framework are to:

- Identify risk across Centrelink (Strategic, Enterprise, Business and Operational);
- Ensure processes are in place to manage risk;
- Embed risk management into existing management frameworks and processes; and

- Involve the whole organisation, from the Centrelink Executive to senior management and employees in order to inculcate and maintain a culture of risk management.

Centrelink's *Risk Management Policy and Guidelines* were developed in accordance with *AS/NZS 4360:2004 Risk Management Standard* and endorsed by the Centrelink Executive.

For the purpose of this plan, fraud risks are identified through the risk assessment process. The risks and control activities that are identified during this process are listed in the individual *Fraud Control Action Plans* and in the sections of this plan that relate to administrative, internal, information and payment fraud.

5.6.1 FRAUD RISK ASSESSMENTS

In accordance with the *Commonwealth Fraud Control Guidelines 2002* Centrelink conducts fraud risk assessments every two years on its major payments and processes and new policy proposals.

The risk assessment process identifies and measures the risks associated with fraud against Centrelink (information and administrative fraud) and the payments administered by Centrelink on behalf of client departments (payment fraud and internal fraud).

The *Commonwealth Fraud Control Guidelines 2002* lists the core areas that must be considered in risk assessments.

The responsibility for assessing fraud risks within Centrelink ultimately lies with the Chief Executive Officer, however, through the fraud governance arrangements, responsibility has been delegated as follows:

Fraud Risk Assessment	Position Responsible
Administrative and Staff Fraud	• Chief Financial Officer, Finance Division • General Manager, People and Ministerial Division • General Manager, Audit, Governance and Assurance Division
Information Fraud	• General Manager, Corporate IT Systems Division • Chief Financial Officer, Finance Division
Payment Fraud	• General Manager, Audit, Governance and Assurance Division • General Manager, Families, Seniors and Business Integrity Division • General Manager, Education, Employment and Support Programs Division

5.7 REPORTING FRAUD TO CENTRELINK

In March 2008, Centrelink implemented a new system for the recording and processing of public allegations of welfare fraud. The new system is known as the Report a Suspected Fraud system.

Fraud can be reported to Centrelink through a number of channels including telephone, in writing or via the Internet. To report a fraud to Centrelink:

- Contact the Australian Government Services Fraud Tip-Off line on **13 15 24;**
- Visit the Centrelink web site at **www.centrelink.gov.au** and report on-line; or
- Write a letter to or visit any Centrelink Customer Service Centre.

5.8 REPORTING FRAUD WITHIN CENTRELINK

Centrelink employee's are required to report all suspected cases of administrative fraud to either their Office Manager/Business Manager, Area/National Manager, Internal Assurance Section, People and Ministerial Division, or in the case of internal program fraud, to the Business Integrity Network Intelligence Section. If employees do not report a suspected fraud, they may be guilty of committing an offence.

There are certain reporting procedures in place that must be followed once an internal fraud is reported or suspected. As all cases are considered serious, particular care must be taken in determining the correct course of action.

The instructions for employees and the correct procedures for reporting a fraud within Centrelink can be found on Centrenet:
Internal Fraud & Ethics Reporting Suite

6. FRAUD PLAN FOR PAYMENT RISKS

6.1 OVERVIEW

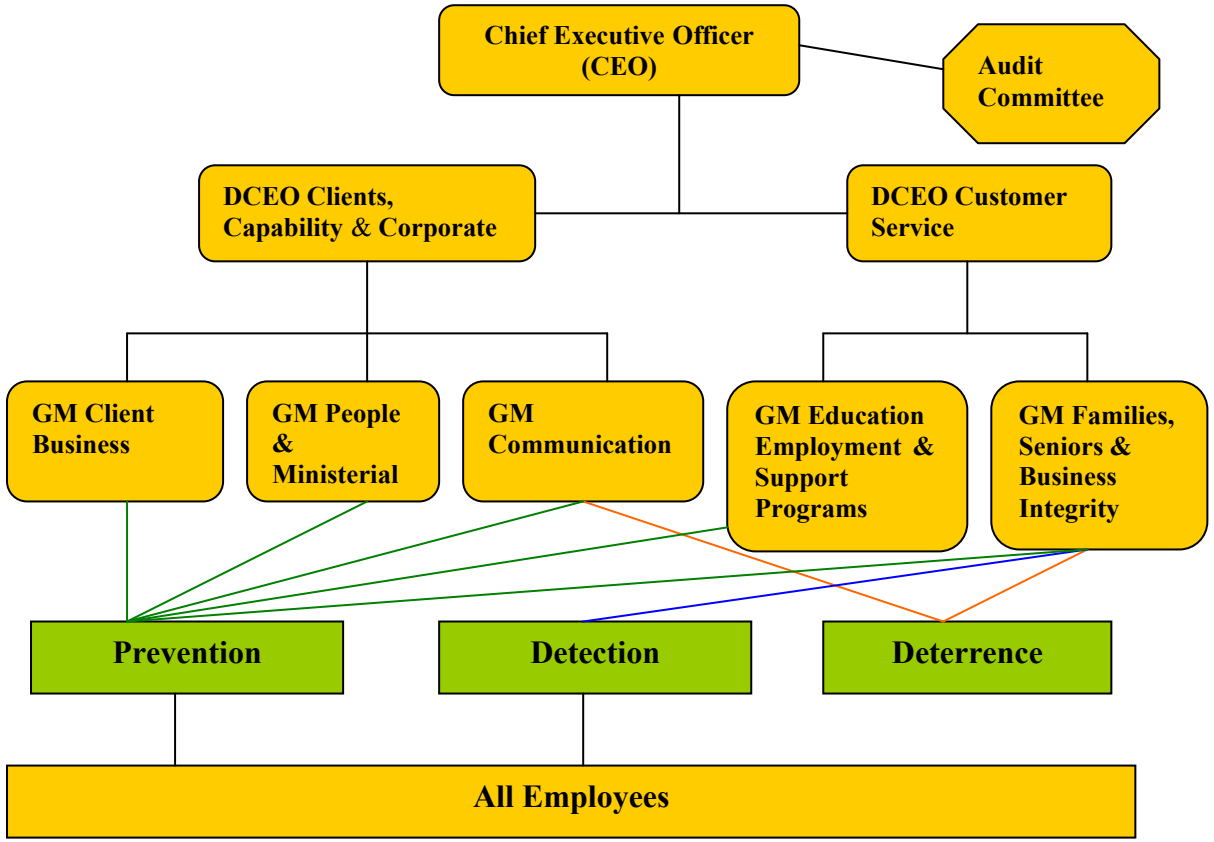
Centrelink operates under a purchaser/provider framework where policy departments and other Government agencies enter into a business partnership or other type of formal agreement with Centrelink. These agreements specify the services or products Centrelink agrees to deliver on their behalf together with the associated funding arrangements. Centrelink provides an annual assurance statement to policy departments to assure them that key risks to its business are being managed effectively.

Agreements with policy departments and other Government agencies provide the majority of Centrelink's funding.

The two agencies that supply the majority of Centrelink's business are:

- The Department of Education, Employment and Workplace Relations; and
- The Department of Families and Housing, Community Services and Indigenous Affairs.

6.1.1 PAYMENT FRAUD MANAGEMENT FRAMEWORK



GM Client Business See table on page 8 for details.	GM People & Ministerial See table on page 8 for details.	GM Communication See table on page 9 for details.	GM Education, Employment & Support Programs See table on page 9 for details.	GM Families, Seniors & Business Integrity See table on page 9 for details.

CEO - Principal responsibility for fraud control within Centrelink and for compliance with the Commonwealth Fraud Control Guidelines.

Audit Committee - Review Centrelink's Fraud Control Plan and satisfy itself that Centrelink has appropriate processes and systems in place to capture and effectively investigate fraud related information. Assist the CEO with responsibilities for financial reporting, maintaining an efficient system of internal controls, improving performance and accountability and reviewing specific matters that may arise from the external audit process.

DCEO Clients, Capability & Corporate – Ensure the integrity of outlays.

DCEO Customer Service – Successfully deliver the Governments employment and social security policy.

6.2 PAYMENT RISK MANAGEMENT

Payment risk management assesses and controls risks to the integrity of payments on behalf of Centrelink's policy departments. When looking at a risk to payment accuracy, Centrelink categorises the causes of risk into customer, administrative or policy/legislation. When examining the payment accuracy issues attributed to the customer then three further levels are applied. Those customers who are considered:

- Uninforme d;
- Unable; or
- Unwilling.

It is this third component that is considered payment fraud. Payment fraud can also involve Centrelink employees. An example of payment fraud is where Centrelink customers and/or employees may knowingly lodge a false claim for payment using a fictitious identity or a known identity, fail to declare circumstances fully, not advise of a change in circumstance or intentionally incorrectly declare income or assets as specified by the relevant legislation. In Centrelink the treatment of payment fraud is not separated from the treatment of payment inaccuracy and as a consequence the following sections will provide commentary on both.

Centrelink is introducing a rolling program of updating payment risk assessments in collaboration with the policy departments. In this way Centrelink can be more sensitive to emerging trends based on regularly updated information. This information can lead to revision of existing control activities or the development of new activities to reduce the risk of incorrect payment and payment fraud closer to the time of identification of a new or changed risk.

Individual controls that address each payment risk are documented in the Payment Integrity Action Plans for each individual program for each Policy Department. Each plan is a living document, which is monitored and updated regularly.

6.3 PERFORMANCE MONITORING AND QUALITY ASSURANCE

Centrelink's Payment Fraud and Compliance performance measures and timeframes for reporting on Fraud and Compliance are set out in the Business Partnership Agreements it has with its various Policy Departments. Performance against the Key Performance Indicators (KPI's) is monitored through an integrated set of performance reports. Feedback from this monitoring is fed back into the Risk Assessment process to allow the updating of risks and to identify new and emerging risks. Centrelink reports on performance against the KPI's by exception to the Policy Departments.

Centrelink produces a comprehensive range of performance data and the Business Integrity Network conducts analysis designed to assist teams achieve the KPI's in place.

6.4 KEY RISKS

The risks contributing to payment fraud have been identified through the formal risk assessment processes. The majority of payments delivered by Centrelink have similar risks, as the basic eligibility requirements are the same.

The following are the risks that are associated with Centrelink payments:

- **Aboriginality**–a customer may falsely claim to be of Aboriginal or Torres Strait Islander origin in order to qualify for payment.
- **Absence from Australia**–customers may leave Australia on a temporary or permanent basis and continue to receive payment.
- **Assets**–assets owned by the claimant, their partner or relevant family members may not be declared or their value understated.
- **Carers**–customer fails to notify cessation of care (for respite, hospitalisation, care receiver dies, change of care, or care receiver permanently enters an institution).
- **Childcare**–Child Care Benefit may be claimed for a period of time when a child was not in care or using care that is not consistent with details on receipts or records lodged by the service, or a service provider may make false claims relating to care provided for children at 'risk'. A childcare service/carer may also claim for Child Care Benefit for children who have never attended or ceased to attend childcare and/or a childcare service may overstate their hours of operation.
- **Compensation**–non-disclosure of past or present compensation payments may result in large overpayments and/or failure to recover previously paid entitlements as required by the social security law (for most payments there are special direct deduction, recovery and preclusion rules for the treatment of compensation).
- **Dependants**–payments for dependent children are no longer payable where the person loses legal responsibility.
- **Dual Payments**–one person may claim two or more payments that are mutually exclusive (e.g. Age Pension and Veterans' Affairs Service Pension).
- **Educational Institutions**–attendance at an educational institution may cease or vary and enrolment at an educational institution may cease or the hours of enrolment or workload may vary.
- **Fitness for Work**–this may impact eligibility for disability related payments and add-ons (Sickness Allowance, Newstart Incapacitated, Youth Disability Supplement, Disability Support Pension).
- **Geographic isolation**–physical isolation may be incorrectly stated in order to qualify for payment.
- **Identity**– fictitious, stolen, lent or manipulated identities for customers and/or dependent children may be used to obtain payment; and fictitious, stolen, lent or manipulated identities may also be used by customers for employment purposes.

- **Imprisonment**–eligibility is precluded during most periods of imprisonment (except for customers in receipt of Lawful Custody Allowance).
- **Income**–a source of income of the claimant, their partner or relevant family members may not be declared, or the amount received may be understated.
- **Independence Status**–a customer receives a higher rate of payment if they are considered to be independent.
- **Maintenance**–customer fails to advise maintenance changes.
- **Marital Status**–a marriage-like relationship precludes eligibility for Parenting Payment Single and is relevant to the means testing of payments generally.
- **Participation/Work Efforts**–customers may falsely declare that they are participating or making efforts to find employment.
- **Payment after Death**–payments may be made to a customer's account after they have died.
- **Residence**–Australian residents without the correct legal status, or failing to meet the required waiting periods, are not eligible for payments and cards.

6.5 CONTROLLING PAYMENT RISK - STRATEGIES AND ACTIVITIES TO PREVENT PAYMENT INACCURACY (INCLUDING FRAUD)

The following overarching preventative strategies and activities address the risks outlined in section 6.4. Specific controls for the individual risks are listed in the Payment Integrity Action Plans.

6.5.1 BUSINESS INTEGRITY STRATEGY

The business integrity strategy being pursued by Centrelink is aimed at enhancing its ability to assure stakeholders and Australian taxpayers that it is providing value for money in its administration of programs. The strategy's aim is to strengthen the preventative controls to reduce the number of incorrect payments, where it is cost effective to do so. The strategy is based on:

- Working with policy agencies to develop an integrated set of Key Performance Indicators (KPIs) that recognise the prevention of incorrect payment as well as the detection of non-compliance;
- Examining Centrelink's interactions with customers to assess, on the basis of evidence, at what point(s) our efforts should be concentrated; and
- Reviewing Centrelink's processes to integrate them and make best use of available resources.

This strategy is:

- Responding to Australian National Audit Office and other concerns expressed that Centrelink should consider devoting more effort to preventing incorrect payments so that less effort will be needed for finding and addressing them after the event;
- Aimed at demonstrating to stakeholders Centrelink's capacity to provide 'value for money';
- Enabling Centrelink's resources to target particular risks exist and/or opportunities to get best value for money; and
- Benefiting customers by preventing incorrect payments and minimising possible debts.

While the strategy is in its early stages, impacts have already been seen in initiatives to produce more cost effective ways of operating.

6.5.2 GETTING IT RIGHT

Centrelink has specific procedures in place for processing new claims, making decisions and conducting reviews.

'Getting it Right' is an element of Centrelink's Business Integrity Strategy and sets the framework for improving accuracy and accountability in Centrelink. It reduces the potential for opportunistic fraud by customers caused by administrative error. This strategy requires all employees within Centrelink including Customer Service Officers, managers, team leaders and specialist officers, to work together to improve accuracy, recording and accountability in their work.

The 'Getting it Right Program' establishes minimum standards for key aspects of Centrelink's operations. These include proof of identity procedures, protocols for recording online documents, and file management.

Under the program, there is increased awareness of the need for employee training and knowledge (see paragraph 6.5.7) of the payments available to customers and ensuring that appropriate claim forms, letters and information products are issued.

6.5.3 TIERED PROOF OF IDENTITY MODEL

Centrelink uses a Tiered Proof of Identity Model. This model gives increased assurance of the proof of identity documents that are provided by Centrelink customers thus helping to reduce the incidence of identity fraud. The customer's proof of identity information is better protected and the requirements of any future proof of identity related business opportunities are met.

The Tiered Proof of Identity Model is consistent with the 'Whole of Government Framework' for proof of identity that involves a range of public sector agencies, including Centrelink, working in conjunction with each other to develop a proof of identity framework that can be applied across agencies. The Tiered POI framework is consistent with the National Identity Security Strategy.

6.5.4 DEBT SERVICING

Centrelink places a strong emphasis on a wide range of debt prevention measures in its dealings with customers and policy agencies. The aim of this action is primarily to prevent or minimise the effect of payment debt to the customer and to increase customers' awareness in notifying of changes in their circumstances to ensure payment correctness to the customer. The role is managed by the Debt Support Services team in NSO with strong leadership to Debt Management Coordinators located in each Area Office.

The role of the Debt Support Services team is:

- To coordinate the national debt management network;
- To develop comprehensive Management Information tools to report and analyse all aspects of Centrelink debt activity and to account authoritatively to our internal and external customers on debt management, trends and resolution strategies;
- To manage internal communication strategies;
- To recommend changes to Centrelink processes, products and procedures to improve correctness, accuracy and to reduce debt as a result of debt management activity, project review and analysis;
- To develop, implement and manage a national debt management database which records and reports all early intervention ongoing activities and projects; and
- To develop and implement national early Intervention and detection strategies for specific customer groups in conjunction with internal and external stakeholders.

6.5.5 INFORMATION TO CUSTOMERS

Fraud prevention includes ensuring that Centrelink customers are provided with information on their rights and obligations. Providing clear and concise information, particularly at the pre-grant stage, reduces the risk of customers failing to advise of changes in their circumstances that may affect their entitlement.

Where appropriate, information about fraud prevention is included in information products provided by Centrelink. Information products assist in both deterring and preventing fraud as customers contemplating fraud are informed that Centrelink does not accept the abuse of payments and that compliance activities are regularly undertaken as a high priority.

Centrelink is regularly updating and providing new information and products to ensure that all customer groups are kept informed of their rights and obligations. These include:

- Customer information seminars;
- Having products that are easily accessible in all Customer Service Centres;

- Ensuring that appropriate pamphlets, fliers and claim forms are provided at the pre-grant stage;
- Providing information products in various languages and offering interpreting services;
- Issuing online advices which include rate of payment, rights and obligations and prosecution information; and
- Centrelink's periodic publications including:
    1. *Rural News* (a magazine for people living in rural and regional Australia);
    2. *News for Seniors* (a direct mail newspaper for age pensioners and Commonwealth Seniors Health Card holders);
    3. *Australian Pension News* (a direct mail newspaper for Australian pensioners living overseas);
    4. *News for Carers* (a direct mail newsletter for Carers); and
    5. *The Journey* (a quarterly publication direct mailed to organisations servicing multicultural customers).

Centrelink also provide specific information in a range of languages on SBS radio and in the major ethnic print media. Translated information products are available in approximately fifty languages that can be issued directly to customers or accessed through the Centrelink website at **www.centrelink.gov.au**.

6.5.6 INFORMATION TO EMPLOYEES

See Section 2.1.3.

6.5.7 EDUCATION AND TRAINING OF EMPLOYEES

The National Learning Strategy provides the strategic framework for the development and delivery of all training and learning activities in Centrelink. The strategy advocates a reference based approach to learning supported by behaviourally based core skill training and the development of career pathways and mobility through qualifications and structured training programs.

See also Section 5.5.

6.6 STRATEGIES AND ACTIVITIES TO DETECT PAYMENT INACCURACY (INCLUDING FRAUD)

The following detective strategies and activities address the risks outlined in Section 6.4.

6.6.1 COMPLIANCE REVIEWS

Compliance reviews are detection measures, which address the risks of incorrect payment identified by Centrelink's payment risk assessments.

A compliance review is conducted where specific information, not previously known and/or not provided by the customer, indicates that an incorrect payment may have occurred. The incorrect payment will usually be a result of error, omission, misrepresentation or fraud on the part of the customer, but may also be caused by error or fraud by employees.

A compliance review is usually triggered by information from an external source or third party or initiated by compliance review employees. External sources of information include other departments or agencies, whose data is matched with Centrelink data to identify cases for review, and tip-offs from members of the public.

6.6.1.1 Department of Immigration And Citizenship (DIAC) Data Matching

From 1 July 2008, every new claim for any Centrelink payment or concession card will be checked electronically with DIAC. DIAC will automatically notify Centrelink of individual changes (departures from Australia, returns, visa changes) that will then result in automatic update of Centrelink customer details.

6.6.2 SERVICE PROFILING

Service profiling is the use of sets of characteristics that identifies and links customers to the most appropriate service strategy for meeting customer and program outcomes.

Service profiling enables Centrelink to identify the most appropriate pattern of customer contact based on the risk that the customer will not achieve relevant program objectives. This enables Centrelink to better target contact with customers, recognising that not all customers require the same level of service and support. Service profiling also determines the intensity and frequency of the contact a customer will have with Centrelink.

6.6.3 ANALYSIS

Centrelink analyses data from various sources to try to determine root causes of error and to recommend strategies for improvement. This includes analysis of Random Sample Survey results and examination of data on debts and debtors to determine if there are any risks that require further review and/or pilot activity with a predominant focus on debts prevention activity.

6.6.4 INVESTIGATIONS

Centrelink conducts various investigations into instances of payment fraud. The form of investigations that are conducted depends on the type of fraud that is committed. These may vary from internal investigations to outsourcing the investigation to an external agency. All investigations that are conducted by Centrelink are in accordance with the *Australian Government Investigations Standards (AGIS)*.

6.6.5 FRAUD INTELLIGENCE

Centrelink has strengthened its ability to detect and investigate serious and complex instances of fraud through the introduction and on-going enhancement of an information collection, analysis and dissemination strategy. Namely, a fraud intelligence capability with the ability to strategically, operationally and tactically analyse information.

- Strategic Intelligence provides insight or understanding, contributing to decisions on broad strategies, policies and resources, directed to achieving medium and long-term organisational goals.
- Operational Intelligence produces targeting opportunities by identifying classes or groups of individuals that fit into certain patterns of activity.
- Tactical Intelligence supports front-line investigations in taking specific action to develop cases to a point where on the balance of probabilities, there is a likelihood of fraud or criminal activity.

Centrelink's intelligence led investigation model enables the assessment of the seriousness and priority of fraud investigations in accordance with the Heads of Commonwealth Operational Law Enforcement Agencies (HOCOLEA) *'Overarching principles for selecting cases for investigation and administrative, civil and criminal sanctions'*.

6.6.6 IDENTITY CRIME

In accordance with the recommendations of the Australasian Centre for Policing research, Centrelink defines identity crime as establishment of fraudulent claims based the use of:

- Fictitious identity;
- Stolen identity;
- Lent identity; and
- Manipulated identity.

The methodologies used to circumvent Centrelink's control measures are often sophisticated and the detection of identity related crime requires the use of specialised skills and tools.

Centrelink rigorously pursues cases of identity related crime in conjunction with the Australian Federal Police (AFP) and the Commonwealth Director of Public Prosecutions (CDPP). All cases of dual or multiple payments are referred to the CDPP with a recommendation to prosecute.

In addition to the detection and co-ordination of investigation of identity related crime cases, Centrelink:

- Develops and implements new detection methodologies and techniques to counter the increasingly sophisticated nature of identity related crime;
- Reports on the risk of exposure to identity related crime;
- Assists in the development of preventative strategies, particularly in the area of new claim admission procedures; and

- Assists in the development of automated 'Watchdog' systems to provide timely indications of possible new frauds.

6.6.7 OUTPOSTED AUSTRALIAN FEDERAL POLICE AGENTS

To enhance the relationship between Centrelink and the AFP**,** the AFP may outpost Federal Agents. The duration of the outposting will vary depending on the AFP and Centrelink's needs. These Federal Agents assist Centrelink by:

- Facilitating the referral of appropriate matters to the AFP for investigation;
- Assisting with investigations of allegations of breaches of legislation for which Centrelink has responsibility;
- Providing and coordinating the training of Centrelink employee's in fraud investigation and related matters; and
- Promoting communication and a better understanding between the AFP and Centrelink.

6.7 STRATEGIES AND ACTIVITIES TO DETER PAYMENT FRAUD

The following strategies and activities address the risks outlined in Section 6.4.

6.7.1 MEDIA EXPOSURE

The Communication Division's role in fraud control is one of prevention and deterrence. The strategies put in place are designed to increase the public's awareness of the consequences involved when a customer is caught obtaining Centrelink payments or services to which they have no entitlement. The Division also aims to promote Centrelink's capacity to detect and investigate suspected fraud.

In consultation with the Minister's Office, Families, Seniors & Business Integrity Division and, when appropriate, the Privacy & Information Access Section, the Communication Division may release information about fraud investigations and surveillance video footage to the media to make the public aware that Centrelink is vigilant against those who try to defraud Centrelink.

Centrelink actively seeks to promote prosecution activity in the media, both locally and nationally. The promotion of this activity enables Centrelink to draw on successful prosecutions as a deterrent measure for those customers who may consider that failing to meet their obligations carries no detrimental effects.

Media releases are also produced and are aimed at deterring those who may be contemplating fraudulently claiming a Centrelink payment. This involves compiling statistics or case studies into a package for media outlets and individual journalists. Such activities seek to highlight the role the community can play in helping Centrelink keep the system fair, by discussing the Australian Government Services Report a Suspected Fraud system. They also reinforce to the Australian taxpayer that their taxes are being well guarded and used for the intended purposes.

6.7.2 DEBT RECOVERY

Debt recovery plays an important role in deterring future instances of fraud. Centrelink has various recovery methods in place that can be applied to effectively recover excess payments from current and non-current customers.

There are specialist recovery units located in the Area Support Offices that are responsible for recovering Centrelink debts.

Once a debt has been identified and the current or non-current customer is advised, there are several tools available for recovery. The use of automatic withholdings from a current customer's fortnightly payment is an effective recovery option to recover the debt as quickly as possible.

In circumstances where other recovery methods have not proved feasible or satisfactory, Centrelink may garnishee wages, tax refunds, bank accounts, impose penalties, refer the debt to an external agency for recovery or apply a mortgage/caveat on property.

6.7.3 PROSECUTIONS

The prosecution of individual cases of fraud against the Australian Government is an integral part of the *Commonwealth Fraud Control Guidelines 2002.* The prosecution of serious offences by customers or employees is important for the deterrence of future instances of fraud.

Information obtained or received by Centrelink may indicate that an offence has been committed under the legislation administered by Centrelink, the *Crimes Act 1914* or the *Criminal Code Act 1995*. Centrelink's role in the prosecution process is to conduct investigations and to refer appropriate cases to the Commonwealth Director of Public Prosecutions (CDPP). The CDPP considers cases in accordance with the *Prosecution Policy of the Commonwealth*. All cases investigated by Centrelink are prepared for prosecution in accordance with the *Australian Government Investigations Standards*.

Centrelink, in conjunction with the CDPP, has developed *National Case Selection Guidelines* for the identification of cases that are considered suitable for possible prosecution.

Centrelink has specialised Fraud Investigation Teams strategically located in major centres around Australia. These teams are responsible for the investigation of suspected instances of payment fraud against Centrelink and the management and preparation of briefs of evidence for referral to the CDPP.

7. FRAUD PLAN FOR ADMINISTRATIVE AND STAFF FRAUD RISKS

7.1 OVERVIEW

Centrelink is committed to providing employee's with an environment where they are supported in complying with the Australian Public Service (APS) Values and APS Code of Conduct and continues to promote an ethical workplace culture through a range of fraud prevention and control initiatives. These include:

- Planning for fraud control;
- Conducting fraud prevention and ethics training;
- Developing proactive detection programs; and
- Investigating matters of potential fraud and misconduct.

Administrative and staff fraud occurs when either Centrelink employees or persons outside of Centrelink use resources for purposes other than for which they were provided. It relates to fraud associated with funds, both program and administrative, resources or property owned, held or under the control of Centrelink.

Administrative and staff fraud for Centrelink broadly includes:

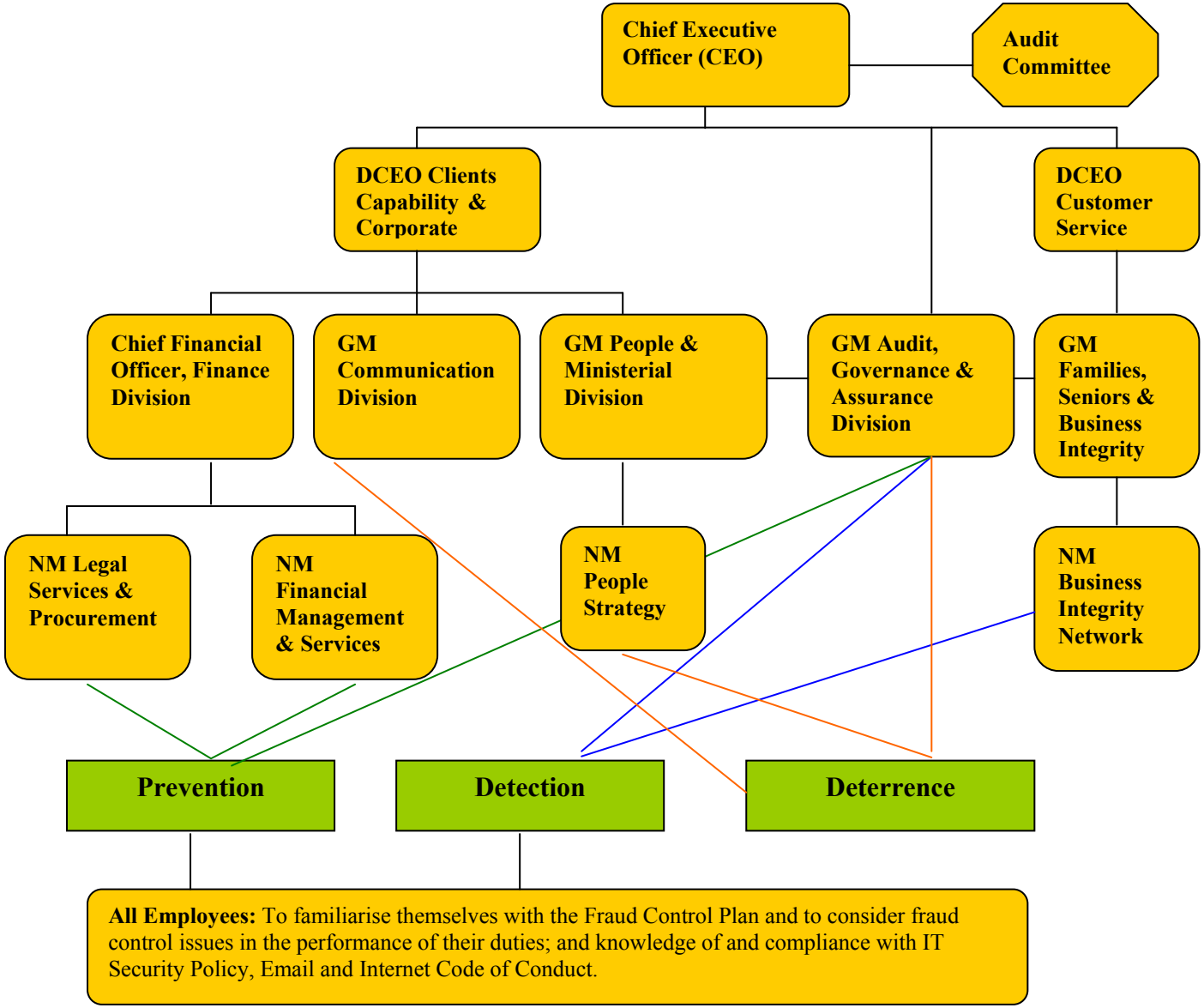
- Theft of Centrelink funds;
- Theft of Centrelink property;
- Misappropriation of Centrelink funds;
- Obtaining a benefit by incorrect recording of data;
- Acceptance of a bribe;
- Making a false claim for an employee entitlement;
- Unlawful use of Centrelink computers, vehicles, telephones and other property or services; and
- Hacking into, or interfering with a Centrelink computer system.

The Internal Assurance Section, Audit, Governance and Assurance Division has responsibility for coordinating the detection and investigation of suspected fraud.

The coordination, review and implementation of fraud control strategies associated with Centrelink employees is the responsibility of Audit, Governance and Assurance Division.

Staff program fraud associated with false and manipulated payment transactions is detected through payment system monitoring carried out by the Business Integrity Network Intelligence Section. The section liaises closely with Area offices and where appropriate Customer Service Centres providing a point of reference for managing suspected staff or administrative fraud.

7.1.1 ADMINISTRATIVE AND STAFF FRAUD MANAGEMENT FRAMEWORK



CEO - Principal responsibility for fraud control within Centrelink and for compliance with the Commonwealth Fraud Control Guidelines.
Audit Committee - Review Centrelink's Fraud Control Plan and satisfy itself that Centrelink has appropriate processes and systems in place to capture and effectively investigate fraud related information. Assist the CEO with responsibilities for financial reporting, maintaining an efficient system of internal controls, improving performance and accountability and reviewing specific matters that may arise from the external audit process.
CFO - Lead and support financial and business capability to satisfy Government expectations and Centrelink's corporate strategy, accountability and legal obligations.
GM, Audit, Governance & Assurance – Provide strategies and processes for preventing, deterring, detecting and investigating internal fraud. Monitors and reviews staff fraud.
NM Legal Services & Procurement – Responsible for ensuring there are appropriate policies in place for all areas of contract management and procurement.
NM Financial Management & Services – Develop policies, procedures and systems to help control financial risk.
Internal Assurance Section – Coordinate the prevention, detection and deterrence of administrative and staff fraud.
NM Business Integrity Network Operations & Finance – Responsible for detection of internal program fraud.
GM People & Ministerial – People Capability & Strategic Planning
NM People Strategy – Code of Conduct Sanctions

7.2 KEY RISKS

There are a number of risk areas for administrative and staff fraud:

- **Advance Payments**–employees may inappropriately reduce the amount outstanding against customer advance payments.
- **Arrears Payments**–employees may deliberately make excessive payments to otherwise legitimate customers.
- **Concession Cards**–employees may inappropriately issue Concession Cards to either customers or themselves.
- **Creation of false customer records**–employees may fraudulently create a false customer record.
- **Credit Cards**–employees may inappropriately use credit or purchasing cards.
- **Debts incorrectly written off**–bad vendor debts may be incorrectly written off.
- **Electronic Benefits Transfer Cards**–Electronic Benefits Transfer Cards may be issued and negotiated by an employee.
- **Email**–employees may inappropriately use email facilities.
- **Fringe Benefits Tax**–employees may reduce the value of reportable fringe benefits shown on the payment summary form.
- **Incorrect assessment of customer records**–deliberate falsification of customer details resulting in an incorrect assessment.
- **Intangible assets**–theft or copying of intangible assets (e.g., intellectual property).
- **Leave entitlements**–leave taken may not be recorded on Infolink, may be incorrectly recorded on Infolink or not authorised.
- **Misuse/Misappropriation**–agency funds may be incorrectly or improperly used.
- **Overpayment of vendor accounts**–collusion between employee's and the vendor.
- **Payments to fictitious vendors**–creation of fictitious vendors and depositing funds into a nominated bank account.
- **Prior convictions and disciplinary action**–applicants may not advise of prior convictions or disciplinary action in previous employment.
- **Purchasing function**–purchasing function may not be performed in accordance with the *Financial Management and Accountability Act 1997.* (Purchase orders raised then goods/services taken by employee.)
- **Record of attendance**–attendance times are different from the flextime recorded.
- **Receipts**–goods may be recorded as receipted when no receipt was given.

- **Recruitment**–bias or conflict of interest in recruitment and selection decisions.
- **Redirection of customer payments**–employees may redirect payments made in the name of genuine customers.
- **Salaries**–salary payments may be incorrect, unauthorised or invalid and/or payroll ghosting.
- **Stores and other consumables**–misuse of stores and other consumables.
- **Tangible Assets**–public property, money or assets may be stolen.
- **Telephones**–employees may inappropriately use desktop telephones and mobile phones.
- **Tenders**–procurement process may be unethical, conflict of interests, inappropriate use of system functions and/or inappropriate relationships with potential bidders.
- **Travel**–travel may not be authorised or undertaken. Travel plans may be changed without the corresponding changes to travel allowance being made. Travel allowance/review travel allowance/remote locality leave fares may be overstated or fraudulent.
- **Vehicles**–employees may inappropriately use Australian Government vehicles.
- **Work history and prior service**–applicants may overstate their work history or educational qualifications or previous history of unsatisfactory employment or prior service may be recorded on Infolink leaving employees with additional credit.

7.3 STRATEGIES AND ACTIVITIES TO PREVENT ADMINISTRATIVE AND STAFF FRAUD

The strategies and activities listed below address the risks outlined in Section 7.2. Specific controls for the individual risks are listed in the Administrative and Staff Fraud Control Action Plan.

7.3.1 INFORMATION TO EMPLOYEES

Centrelink has developed its own financial management manual, which is known as *Money Matters*. *Money Matters* explains the rules regarding public money and property contained in the *Financial Management and Accountability Act 1997* and provides policy and procedures for Centrelink employees. It also lists the penalties associated with offences.

Money Matters is being progressively replaced with a new series of Financial Policy Instructions. The new policy instructions will be displayed on the Financial Policy Index page of Centrenet.

The Spending Approver Tool on Centrenet provides employees with information on spending delegations.

Centrelink also has an Internal Fraud Awareness Kit that details how employee fraud that relates to administrative and program fraud is handled within Centrelink. There is specific information within the site advising employees about ways to report and handle suspected instances of administrative and program fraud. It also includes suggestions for reducing the risk of internal fraud occurring within the workplace.

The Ethics Resource Kit includes a range of information relevant to employee ethical obligations. In particular, the Kit contains Centrelink's Ethics and Conduct Handbook, which brings together a range of information relevant to employee obligations. The Kit also contains the latest edition of the Centrelink Values Newsletter as well as privacy specific documentation and the Centrelink Declaration of Confidentiality booklet.

Staff fraud risks and controls are considered as part of the process applied to all new financial policy under development.

See also Section 2.1.3.

7.3.2 COMMUNICATION STRATEGY

Centrelink has developed a communication strategy that aims to increase employee awareness of the prevention, detection and deterrent strategies in relation to fraud and the consequences of being caught. It reinforces that all employees have a responsibility to act ethically and to seek to prevent administrative fraud and loss. Components of the strategy include managers and team leaders discussing fraud issues with employees, and using various internal mechanisms such as screen savers, open forums and the Centrelink administrative reference suite to send employees fraud and misconduct messages.

7.3.3 SYSTEM CONTROLS

System controls are edits built into the payment systems and Infolink FI and HR systems to help ensure the integrity and completeness of data entered. For example, there are fields that must be completed before processing will occur; screen flows, where after completing one screen, the system automatically determines from the information entered, whether another screen should also be completed.

7.4 STRATEGIES AND ACTIVITIES TO DETECT ADMINISTRATIVE AND STAFF FRAUD

Strategies and activities that address the risks outlined in Section 7.2 are listed below. Specific controls for the individual risks are listed in the Administrative and Staff Fraud Control Action Plan.

7.4.1 TRANSACTIONAL ANALYSIS

Centrelink employees process over 5 billion transactions each year. Centrelink analyses a range of these transactions that fall within the key risk areas for program fraud carried out by employees. Transactions are compared with a range of other data to highlight those transactions considered to be a higher than average risk of being fraudulent. Processes have been automated to continually monitor those transactions requiring further examination.

7.4.2 IDENTITY ANALYSIS

Centrelink has developed a variety of techniques to assess the authenticity of customer identity details. Customers failing to meet certain criteria are selected for further analysis. This can include comparing identity details with the transactional and log data of all employee access.

7.4.3 DATA MATCHING

Centrelink matches data from other Government agencies to highlight customer records displaying identity anomalies. Compliance reviews generated from Data Matching within Centrelink outlined in Section 7.4.1 may also detect staff fraud relating to program funds.

7.4.4 SYSTEM CONTROLS

See Section 7.3.3.

7.5 STRATEGIES AND ACTIVITIES TO DETER ADMINISTRATIVE AND STAFF FRAUD

The following strategies and activities address the risks outlined in Section 7.2.

7.5.1 MEDIA EXPOSURE

See Section 6.7.1

7.5.2 PROSECUTIONS

See Section 6.7.3

7.5.3 PENALTIES

Where an employee is found to have breached the APS Code of Conduct a sanction may be applied. Sanctions include, but are not limited to, termination of employment, reduction in classification, reduction in salary and a fine.

The penalties that can be imposed on a person, on conviction for a criminal offence, vary depending on the type of crime committed and the legislation the crime was committed under but include up to ten years imprisonment and fines.

8. FRAUD PLAN FOR INFORMATION RISKS

8.1 OVERVIEW

Fraud against the Commonwealth is defined as 'dishonestly obtaining a benefit by deception or other means' (see section 3.1).

The *Australian Government Protective Security Manual 2005* defines official information as 'any information developed, received, or collected by, or on behalf of, the Government through its agencies and contractors'.

Centrelink defines Information Fraud as the theft or misuse of information held by Centrelink.

Information Fraud occurs when employees make inappropriate use of information they have access to as part of their duties. Information fraud does not just relate to information regarding customers, it includes any official information as well as unauthorised access to Centrelink's computer systems from people outside the organisation (hackers).

The benefit obtained from Information Fraud may be tangible or intangible. An example of a tangible benefit would be the selling or provision of customer details to third parties (e.g. private investigators). An intangible benefit may be obtaining personal information about a colleague, or others, which you are not entitled to access.

With approximately 6.5 million customers, Centrelink stores a significant amount of information on individuals. In order to effectively manage this information Centrelink has a strong privacy culture. The foundation of Centrelink's privacy culture is its legal obligation to comply with the *Privacy Act 1988* and the confidentiality provisions of the legislation Centrelink administers.

8.1.1 INFORMATION FRAUD MANAGEMENT FRAMEWORK

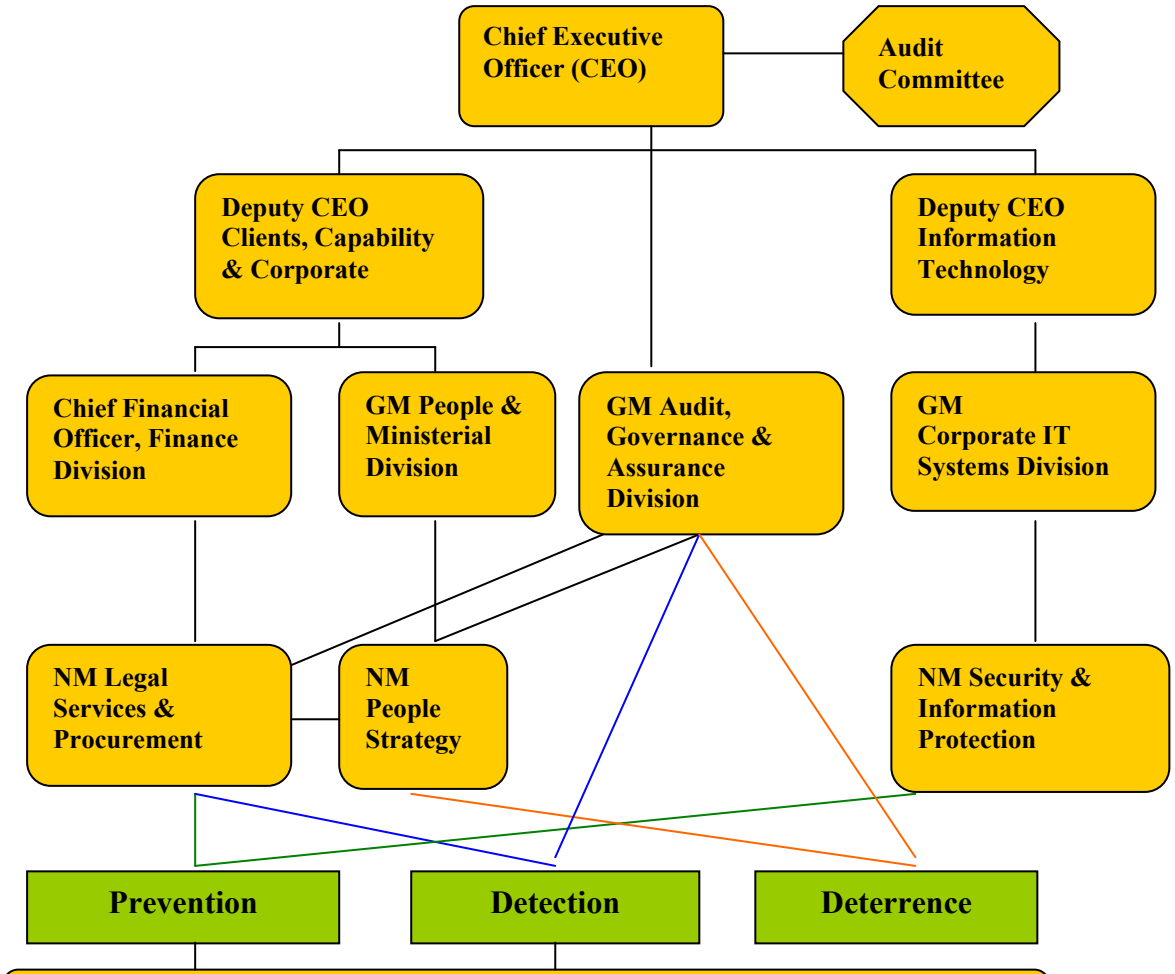
DCEO Clients, Capability & Corporate – Ensure the integrity of outlays.

CFO - Lead and support financial and business capability to satisfy government expectations and Centrelink's corporate strategy, accountability and legal obligations.

NM, Legal Services & Procurement - (through Privacy & Information Access Section) - Develop policy guidelines and procedures and investigates alleged breaches of privacy and confidentiality for referral to code of conduct. Provide advice on privacy, confidentiality and fraud.

GM People & Ministerial - People capability & strategic planning.

NM People Strategy Branch – Code of Conduct Sanctions - (through Sanctions Delegate).



CEO - Principal responsibility for fraud control within Centrelink and for compliance with the Commonwealth Fraud Control Guidelines.

Audit Committee - Review Centrelink's Fraud Control Plan and satisfy itself that Centrelink has appropriate processes and systems in place to capture and effectively investigate fraud related information. Assist the CEO with responsibilities for financial reporting, maintaining an efficient system of internal controls, improving performance and accountability and reviewing specific matters that may arise from the external audit process.

DCEO Information Technology - Ensure that effective IT strategies are in place.

GM, Corporate IT Systems - Provide a security and information protection service.

NM Security & Information Protection - Provide and implement strategies for the protection of Centrelink assets and information and provide security for assets including employees.

GM, Audit, Governance & Assurance – Provide strategies and processes for preventing, detecting and investigating internal fraud (through Internal Assurance Section).

8.2 KEY RISKS

The following are the key risks associated with information fraud:

- **Unauthorised access and use of information** – where a person intentionally obtains (or attempts to obtain) information to which they are not authorised or required to access and/or attempts to alter, delete or otherwise make use of, information to which they are not authorised or required to.
- **Unauthorised disclosure of information** – where a person discloses information (or attempts to disclose information) that they are not authorised to.

8.3 STRATEGIES AND ACTIVITIES TO PREVENT UNAUTHORISED ACCESS, USE AND DISCLOSURE OF INFORMATION.

The following strategies and activities address the risks outlined in section 8.2.

8.3.1 PRIVACY IMPACT ASSESSMENTS

Centrelink, in consultation with the policy department, assesses the impact of any new service that involves personal information holdings or new technologies to ensure that privacy issues are addressed and the privacy compliance program continues to be effective.

8.3.2 PRIVACY AWARENESS KIT

All Centrelink employees are provided with access to the Privacy Awareness Kit through Centrenet. The Privacy Awareness Kit includes:

- The Privacy and Confidentiality Manual – this manual has been developed to assist employee's understand and apply privacy legislation in their day-to-day work to ensure that Centrelink meets its obligations under the *Privacy Act 1988.* The manual also assists employee's to understand and apply confidentiality legislation contained in social security law, the family assistance law and other legislation administered by Centrelink.

- The Authorisations signed by Centrelink's Chief Executive Officer authorising 'Release of Information to other Commonwealth Agencies'; and

- The Ministerial Guidelines that underpin the delegation signed by Centrelink's Chief Executive Officer authorising specific employee's to release information in various 'public interest' categories.

In addition to the Privacy Awareness Kit, Centrelink has developed a suite of Privacy, Confidentiality and Freedom of Information training modules as well as pamphlets, fact sheets, screen savers, videos and posters to ensure employee's are aware of their obligations to protect the privacy of customers and other Centrelink employee's.

8.3.3 DECLARATION OF CONFIDENTIALITY

On commencement of employment, all Centrelink employees must sign a form to acknowledge that they have read and understood their confidentiality obligations. In addition, from January 2008, all employees receive an e-mail requiring them to acknowledge their confidentiality obligations on commencement and then annually on their commencement anniversary.

Employee's are required to acknowledge that they have read, understood and agree to abide by the rules contained in the Declaration of Confidentiality - Privacy, Security, Fraud Awareness and Conduct Responsibilities booklet.

8.3.4 DENY ACCESS FACILITY

The Deny Access Facility (DAF) is available for those customers who have genuine fears for their safety. It was introduced to provide additional security to the records of these customers.

DAF only offers protection from inappropriate access to a person's computer records by Centrelink employees, by effectively denying access to a customer's computer record to the majority of employee's.

Customers who may be eligible to be granted this additional protection of their personal information are customers:

- Who are escaping domestic/physical violence; or
- Who are under police protection and are in life threatening situations; or
- Fleeing involvement in cults or religious sects; or
- Where a privacy or confidentiality breach has been substantiated or where a privacy or confidentiality breach is under investigation.

The paper files of a customer granted Deny Access status are securely stored [redacted]

8.3.5 CUSTOMER PASSWORDS

A customer authentication password is another computer based security measure that is available to customers who are concerned about their privacy. A password is created by the customer and appears once the customer's record is accessed. The customer is then asked to verify their identity by

telling the Centrelink employee (usually a Customer Service Adviser) their nominated password.

This helps circumvent unauthorised persons misrepresenting their identity in order to obtain confidential customer information.

8.3.6 CLEAR DESK POLICY

The Clear Desk Policy was introduced to minimise the amount of sensitive information that is accessible or visible on an employee's desk. Centrelink employees must ensure that all sensitive information, including customer and employee related files and other valuable assets are secured appropriately when they are absent from the workplace.

8.3.7 CHIEF EXECUTIVE INSTRUCTIONS

Chief Executive Instructions (CEI's) are an important governance mechanism by which the CEO prescribes Centrelink's policies and procedures.

CEI 20 relates to the unauthorised access to Centrelink customer records and the personnel records of Centrelink employees. The purpose of the CEI is to clearly articulate Centrelink's rules regarding unauthorised access to the personal information of Centrelink customers and employees.

CEI 21 relates to Centrelink employees interacting with Centrelink as customers. The CEI is in place to protect the privacy of our customers and employees and to protect employees from unfounded allegations regarding unauthorised access to personal information.

CEI's - Table of Contents

8.3.8 PROCUREMENT PROCESS

Probity protocols are built in to Centrelink's complex procurement processes (either in the probity guidance, probity protocols or set out in the tender evaluation plan). Templates that are provided on the Procurement Branch intranet page can include deeds of confidentiality from contractors or can address other specific risks identified on a case by case basis.

Potential information fraud by contractors is managed by seeking deeds of confidentiality under the contract from the contractor and, where necessary, key personnel doing the work. A proforma is usually included in contracts valued at over $80,000. Also, legal and probity advice is often obtained during the procurement process and this acts as an additional control.

8.4 STRATEGIES AND ACTIVITIES TO DETECT UNAUTHORISED ACCESS, USE AND DISCLOSURE OF INFORMATION.

The following strategies and activities address the risks outlined in section 8.2.

8.4.1 CUSTOMER RECORD ACCESS MONITOR

It is a Centrelink requirement that all access to Centrelink's Income Security Information System is logged. The purpose of this log is to provide an audit base detailing access to customer records. The information held in the log may be used to investigate allegations of a breach of confidentiality or suspected fraudulent activities.

Information held includes:

- The customer record details;
- The user identification of the employee accessing the record;
- The date the record was accessed;
- The time the record was accessed; and
- The screens that were accessed.

Chief Executive Instruction (CEI) 16 is the authority used to prescribe the requirement that all customer data must be logged to CRAM.

8.4.2 SECURITY INCIDENTS

It is essential to identify and address security incidents to ensure employee safety and the safety of customers within the Centrelink environment.

All employees who access official information and/or resources have a personal responsibility to report security incidents.

These incidents include (but are not limited to):

- Damage to Australian Government property (including the result of customer aggression);
- Criminal actions such as theft, break and enter, vandalism or assault;
- Natural occurrences such as fire or flood, which could compromise the security of Centrelink;
- Building evacuations and/or receipt of suspicious mail item;
- Negligent handling of security classified information such as not providing the required protection during transfer or transmission, not storing security classified information in an appropriate security container, not properly securing keys or security containers (for example, emailing of Cabinet-in-Confidence information without encryption, or not storing this information in a Class B security container);

- Accessing official information without authorisation (an example of this is accessing Cabinet-in-Confidence information without a PROTECTED level security clearance);
- Sharing official information with a person who is not authorised to access it (for example, passing Cabinet-in-Confidence information to someone who does not have a PROTECTED level security clearance);
- Sharing logon ids and passwords, or allowing another employee to use your computer access; or
- A general security concern within an office.

Information provided about security incidents, and information obtained during the course of security investigations is appropriately secured and is accessed only by employees with a need to know. Employee's can report a security incident by using the online report that can be accessed through the Security and Information Protection Branch Homepage on Centrenet.

Chief Executive Instruction (CEI) 2 is the authority used to prescribe that all security incidents must be reported.

8.4.3 INVESTIGATION OF SUSPECTED PRIVACY BREACHES

All privacy incidents will be investigated, even where it may involve an accidental or unintentional breakdown of administrative procedures that has resulted in a breach of the Information Privacy Principles or the confidentiality provisions contained in legislation administered by Centrelink.

All allegations are investigated and the outcome documented on file and in Centrelink's electronic Privacy Information Reporting System.

Serious cases of information fraud are referred for Code of Conduct investigation or to the AFP for criminal investigation.

A Centrelink fact sheet has been developed that advises employees of the procedures and their rights should they be asked to participate in a discussion in relation to a privacy investigation. This fact sheet is available online to all employee's at:

Privacy investigation procedures and your rights

8.4.4 PRIVACY COMPLIANCE STRATEGY – BROWSING

Centrelink recognises maintaining privacy is a good business practice and critical to progress customer service. It is vital to maintain public confidence in Centrelink's ability to protect individual privacy.

A control framework of prevention, detection and deterrence of browsing and inappropriate access to customer information is in place in Centrelink.

Refer to Chapter 3.060 of the Privacy and Confidentiality Manual.

8.5 STRATEGIES AND ACTIVITIES TO DETER UNAUTHORISED ACCESS, USE AND DISCLOSURE OF INFORMATION.

The following strategies and activities address the risks outlined in section 8.2.

8.5.1 DISCIPLINARY ACTION

An occurrence of information fraud, whether the benefit is tangible or intangible, may also constitute a breach of the Australian Public Service Code of Conduct. Any employee who breaches privacy or confidentiality can expect Centrelink to take disciplinary action against them. This can result in counselling, a reprimand, reassignment of duties, reduction in classification, reduction in salary, deduction from salary or termination of employment.

8.5.2 PROSECUTION AND PENALTIES

Prosecution under criminal provisions may be pursued where some form of payment is received for providing information to an unauthorised person or company. The *Social Security (Administration) Act 1999,* the *Student Assistance Act 1973*, the *Family Assistance (Administration) Act 1999,* the *Crimes Act 1914* and the *Criminal Code Act 1995* all have very strict criminal provisions against the deliberate and unauthorised access and disclosure of customer information. This can result in penalties such as two years imprisonment or fine.