MINISTRY OF SOCIAL DEVELOPMENT
TE MANATŪ WHAKAHIATO ORA

21 August 2024

Tēnā koe

Official Information Act request

Thank you for your email of 21 June 2024, requesting information about any use of social media monitoring by the Ministry.

I have considered your request under the Official Information Act 1982 (the Act). Please find my decision on your request set out below.

On 22 July 2024, the Ministry notified you that more time was needed to respond to your request. The reason for the extension is that consultations necessary to make a decision on the request were such that a proper response to the request could not reasonably be made within the original time limit.

Key developments

In December 2018, the Public Service Commission Te Kawa Mataaho (PSC) issued its model standards on information gathering and public trust. The Ministry was required to attest that its arrangements complied with the model standards. The attestation was due by 30 June 2019.

In May 2019, the Office of the Privacy Commissioner (OPC) released its findings from the Inquiry into the Ministry's use of Section 11 (Social Security Act 1964) and Compliance with the Code of Conduct. Our actions to address the OPC recommendations focused on fraud and related activities.

Therefore, given the work underway, and with agreement from PSC, attestation in relation to the fraud and related activities, would be provided later. Actions to address the OPC recommendations were implemented between 2019 and 2021.

In May 2021, as part of the internal assurance plan for FY20/21, the Ministry commissioned the Ernst and Young (EY) report. This was part of a wider work programme, following implementation of the Privacy Act 2020, to look at different aspects of the Ministry's information practices.

The EY report highlighted that our practice was not up to standard, and we accepted that.

In June 2021, the Ministry suspended the use of 'pseudo' social media profiles and tightened up our practice by introducing guidance (the guidance) to ensure Intelligence Unit staff used social media to gather intelligence in a manner consistent with practices used for our fraud investigations.

In April 2022, the Ministry commissioned an additional engagement under the assurance plan for January to June 2022. This review, undertaken by Simply

Privacy, focused on the Ministry's compliance with the information gathering and PSC model standards in relation to its fraud related activities.

The Simply Privacy review was commissioned later than expected in light of the Ministry's Integrity and Debt area's ongoing involvement in ensuring the integrity of the Wage Subsidy Scheme.

In early 2023, the Simply Privacy report *External Fraud Information Gathering Policies and Processes* was finalised.

Policy developed

In July 2024, the Ministry's policy (*Use of publicly available information to support the integrity of the welfare system*) was approved, covering how we gather publicly available information, including on social media, further strengthening our processes and controls for all staff working to maintain integrity of the welfare system (the policy).

We are now implementing the policy and it will be in place by the end of October 2024.

We accept that the policy has taken considerable time to finalise. The development of the policy was delayed during Covid-19 because the Integrity and Debt team's primary task over that period became the integrity of the $18.8b Wage Subsidy Scheme.

The policy defines what is considered publicly available information and provides guidance and objectives for the Ministry's Integrity and Debt and Workplace Integrity staff undertaking searches of public sources and is supported by comprehensive guidance around the use of social media accounts, profiles and/or pages.

Accounts, profiles, and pages created on social media platforms for integrity purposes will use names that identify them as being operated by the Ministry, e.g. "MSD Client Service Integrity". These will be used to view publicly available information where we have reasonable cause to suspect a person may have committed an offence.

Where the information is not publicly available information, or the use of publicly available information would be unfair or reasonable, staff cannot collect the information without identifying another legal authority for doing so (such as Schedule 6 of the Social Security Act 2018).

Documents enclosed

The following key documents are provided in the **Appendix**:

- The *Interim Social Media Use Guidelines* (2017).
- An internal advisory review undertaken by Ernst and Young titled *Ministry of Social Development Assessment of Information Gathering Process and Controls* (2021)
- An internal assurance review undertaken by Simply Privacy titled *Ministry of Social Development External Fraud Information Gathering Policies and Processes* (2022).

The rest of your request

The following parts of your request are addressed in-turn (and grouped-up where appropriate):

> *Question 1: RNZ requests release of comprehensive, accurate info including of the most up-to-date kind to enable RNZ to report what the current state of this matter is, in full and in fully searchable and copyable format (where 'document' refers to any kind of document, including report/s, memo/s, business case/s, aide memoir/s, briefing/s, minute/s, update/s, and with any parties including the board, any minister, the executive leadership). Please provide me with all information relevant to that statement and/or decision:*
>
> *The 2021 report as noted in previous emails on MSD information gathering with all attachments and appendices.*
>
> *Pls ensure that all info about the way MSD was using social media (monitoring, data gathering, use of aliases, etc) - prior to the report and subsequent to 2017 interim guidelines - are detailed and not redacted, so it is fully clear what MSD was doing*
>
> *In addition, pls release the key document that covers those outcomes – including changes, pauses, cancellations of ways of info gathering, and/or policies, programmes, procedures*

We have identified a draft table *Advisory review – Assessment of Information Gathering Processes and Controls: Action Plan* in scope of this part of your request, it is included in the **Appendix**.

Alongside the policy, we are also providing you with two adjunct resources in the **Appendix**:

- *Social Media Searches*
- Memo: *Use of publicly available information to support integrity of the welfare system*

The Ministry's Intelligence and Integrity Insights team (formerly the Intelligence Unit) combine intelligence, insights, and analytics to better understand integrity risks across the welfare system.

Other information in scope of this part of your request may also exist within Intelligence and Integrity Insights team internal emails between 2017 and 2021.

In order to identify and provide you with all relevant emails, the Ministry would need to divert personnel from their core duties and allocate extra time to complete this task. The diversion of these resources would impair the Ministry's ability to continue standard operations and would be an inefficient use of the Ministry's resources. As such, your request is refused under section 18(f) of the Act, requires substantial collation.

I have considered whether the Ministry would be able to respond to your requests given extra time, or the ability to charge for the information requested. I have concluded that, in either case, the Ministry's ability to undertake its work would still be prejudiced.

> *Question 2: Pls fully detail the subsequent outcomes arising from that report in any ways they affect interactions of any kind with the public*

Integrity-related engagements with the public, including clients, are conducted by Client Service Integrity staff, including Investigators. Please see attached in the **Appendix** the Ministry's Intranet resource *Investigative Techniques*.

In terms of any outcomes from the *Ministry of Social Development Assessment of Information Gathering Process and Controls* in the context of the Ministry's interactions with the public, the use of social media for this type of information gathering has always been passive rather than active.

Therefore this part of your request is refused under section 18(e) of the Act as this information does not exist.

> *Question 3: Pls provide a dated list of any and all external interactions MSD has had about the matters related to the 2021 report, since 2021, including with the Privacy Commissioner, Ombudsman, any other regulator, any panel or similar with external people set up at MSD in an advisory or oversight or any other role.*
>
> *Pls release any comms (incl electronic and summaries of verbal exchanges) between MSD and any of the above externals, where concerns were raised about MSD info gathering.*

The *Ministry of Social Development Assessment of Information Gathering Process and Controls* report was commissioned as part of the Ministry's internal assurance work programme and was not subject to external consultation or oversight. Therefore this part of your request is refused under section 18(e) of the Act as this information does not exist.

> *Question 4: Pls redact names of junior staff but include those of senior ones*

Senior staff are generally defined as staff that hold a role that sits at tier three or above (the tier three role is commonly a General Manager or a Director level position). In line with this definition, we have withheld any staff names that are tier four or below as they are not considered senior staff and are out of scope of your request. If you want any tier four or below names considered for release, please get in contact with us.

> *Question 5: Details of any data-sharing arrangement with any party external to MSD, by which any of the info gathered from social media is or can be shared, including anything covered by an MOU or MOA, including when it was set up; what info it covers; and include a record of what MSD has in writing about the constraints on how any shared information can be used; and how long it can be retained for by the receiving external.*

Information gathered from social media for integrity purposes is not in scope of the Ministry's information sharing arrangements with other agencies. Therefore this part of your request is refused under section 18(e) of the Act as this document does not exist.

Some information in the **Appendix** has been withheld as out of scope of your request.

Some information in the **Appendix** is withheld under section 9(2)(h) of the Act in order to maintain legal professional privilege. The greater public interest is in ensuring that government agencies can continue to obtain confidential legal advice.

Some information in the **Appendix** has been withheld under section 6(c) of the Act where making that information available would be likely to prejudice the maintenance of the law, including the prevention, investigation and detection of offences.

Some information in the **Appendix** has been withheld under section 9(2)(g)(i) of the Act to protect the effective conduct of public affairs through the free and frank expression of opinions. I believe the greater public interest is in the ability of individuals to express opinions in the course of their duty.

I will be publishing this decision letter, with your personal details deleted, on the Ministry's website in due course.

If you wish to discuss this response with us, please feel free to contact OIA_Requests@msd.govt.nz.

If you are not satisfied with my decision on your request, you have the right to seek an investigation and review by the Ombudsman. Information about how to make a complaint is available at www.ombudsman.parliament.nz or 0800 802 602.

Ngā mihi nui

Magnus O'Neill
General Manager
Ministerial and Executive Services

Appendix

MINISTRY OF
SOCIAL DEVELOPMENT
Te Manatū Whakahiato Ora

Organisational Security Intelligence

Interim Social Media Use Guidelines

March 2017

Owner:	Out of scope
Author:	Out of scope
Version:	**1**
File Ref:	**fA1206899**
Release date:	**29 March 2017**

Sign off

This form records the approval and acceptance of the following document:

Document Name	Version	EDRMS File Reference
Interim Social Media Use Guidelines	1	fA1206899

The following signatures indicate approval and acceptance of the above document, subject to any caveats below.

Name	Role	Signature/Date
Merv Dacre	Associate DCE, Corporate Solutions	_____ ____/____/____
Caveats: …… ……		
		_____ ____/____/____
Caveats: …… ……		

Distribution List

Version	Date	Author	Distributed to	Comments/Feedback
1	29/03/2017	Out of scope	Merv Dacre	

Table of Contents

Purpose

This document details the process and guidelines that the Organisational Security Intelligence Unit (Intel Unit) will follow when collecting information from social media platforms, when looking for indicators of benefit entitlement and fraud.

Users of guidelines

These guidelines will be followed by all employees in the Intel Team, who are either based at National Office, or who are on secondment, both within the Ministry and outside with other agencies. If an analyst is representing the Ministry within an intelligence function, these guidelines should be followed.

The collection of information from social media will only be undertaken for MSD related purposes i.e. reviewing benefit entitlement and serious threat against the Ministry.

Background

New Zealanders are becoming increasingly more active online, with the majority of people using social media platforms to share personal information (relationships, family and employment), photographs and views.

Analysts within the Intel Unit use a range of social media platforms to look for indicators of fraudulent activity committed against the Ministry, and assessing the behaviour of high-risk clients.[1]

The information that is available from these sources can be vital for the purposes of intelligence gathering; assessing benefit entitlement and assisting investigations.

Currently there is no broad Ministry operational policy around the use of social media. Design and Improvement Fraud have published limited guidelines around the use of Facebook for investigations However these do not meet the requirements of the Intel Unit.

Levels of searching

In 2014, the Australia New Zealand Policing Advisory Agency (ANZPAA) produced a report that identified five roles carried out by Police staff acting as Online Practioners. The roles reflected the different online actions that the practioners would take (from scanning through to interacting with the person of interest), and the tools they used.

When looking at the model below the Intel Unit currently fits within level three “Discreet Online Persona”.

[1] Intel Team are tasked on occasion by Health, Safety and Security to conduct risk assessments on high risk clients.

This level facilitates analysts to acquire information on a particular person, which then can be built into an intelligence product. Analysts fulfilling this role will use a "persona" to mitigate the risk of leaving a footprint behind, and potential identification by the person they are looking into. This level (for the Intel Team) will not go to the extent of using a stand-alone computer to hide their IP address.

Passive user vs. Active user

The Intel Unit, in its use of social media are deemed currently to be "Passive Users" when collecting information. A passive user describes an analyst who logs onto a particular platform (either using their own personal account or a fake persona) to access specific information for intelligence or investigative purposes.

The analyst does not engage or interact with the people they are collecting information on. If the information is not publicly available (once logged in) the analyst does not go further to try and source it.

By being a "Passive User" when collecting information, the Intel team are abiding by Principle Four of the Privacy Act (manner of collection of personal information). Only publicly available information will be collected. Analysts will not engage in misleading behaviour to collect private information. Thus, they are not collecting information through a manner that is deemed unlawful, unfair, or unreasonably intrusive.

Collection of information

Advice from the Office of the Privacy Commission, regarding the collection of information from social media, states:

Anyone can generally collect photos and personal information about other people from social media for their own personal use. But in other contexts, businesses and organisations should:

1. Only collect information that is necessary for them to carry out their relevant functions (information privacy principle one),
2. Get it directly from the person concerned where practicable (information privacy principle two), and

3. Take care not to be unfair or unreasonably intrusive when doing so (information privacy principle four).

These three principles mean that collecting information about someone from publicly available social media when you have a genuine need for that information, and you can't get it directly from the person, is not an issue. Accessing a publicly available social media profile is not considered unreasonably intrusive, since it is information that anyone can see.[2]

There are three ways in which an analyst would show a genuine need to collect information from social media. This is an either through an open investigation, a detailed Data Mining Project plan, or an imminent threat situation developing. 6(c)

The introduction of the Harmful Digital Communications Act (2015) amended two Privacy principles (10 and 11). This now means that "public availability" of information is no longer a complete exception to privacy. When someone uses or distributes information that was already in the public domain and the use or disclosure harms the individual, the user can be found liable for breaching principles 10 and 11.

For the Intel team, this has an impact on where the analysts collect the information. Pictures and comments must be taken from the person (or people) under investigation. The person (or people) must have posted it themselves and not simply be tagged in the picture or comment. This will ensure that the information collected has been made public from the source and source alone.

Social media platforms used to gather information

Five main social media platforms have been identified by the Intel Unit as being useful for sourcing information for intelligence purposes. As noted with these platforms, they have clear rules and regulations around using false information. These platforms are:

- Facebook
- Linked In
- You Tube
- Twitter
- Instagram

Annex A lists the Terms and Conditions from the above platforms.

Facebook is the main platform that analysts use to collect information for intelligence products. It is the most successful in 6(c)

Their terms and conditions state that users are to provide their real names and information. No false personal information should be provided on Facebook, nor should accounts be created for anyone other than the person using the platform.

[2] https://privacy.org.nz/further-resources/knowledge-base/view/348

LinkedIn is a platform for professionals to create profiles that can be marketed to other professionals and companies. Currently the service has 467 million members in over 200 countries. This service is good for finding information 6(c)

Their terms and conditions also state that a person will only have one account, which must be in their real name.

YouTube is a platform that allows billions of people to watch a range of videos. It allows people to connect to others and share clips of all subjects. This is the one of the lesser platforms used by Intel, but on occasion can be useful.

In their terms and conditions it states you must provide accurate and complete information.

Twitter is a platform that allows users to post and read short (140 character) messages called 'tweets'. To write a tweet, you must be registered to the site. However unregistered users can still see tweets. However when an analyst uses this site to search for a particular person and tweet, they must be logged into the site. This is one of the lesser sites used in the Intel unit.

Twitter's terms and conditions have a clear mandate around the use of impersonating others in a manner that is intended to, or does mislead, confuse, or deceive others.

Instagram is an online mobile photo-sharing site that allows users to share short videos and pictures "publicly" or privately with selected friends. Users can connect their Instagram account to other social media platforms; Facebook, Twitter, Tumblr and Flickr. This results in a photo or video being shared across numerous sites.

In their terms and conditions, they clearly state that creation of accounts must be true and users are prohibited to create accounts for others. All information upon registration must be true, accurate, current and complete.

Identified risks

The primary risk identified in the Intel Unit's practice of using social media for intelligence purposes, is that we are currently breaking the terms and conditions for the different platforms when using a false account.

Each platform state that when someone misrepresents themselves through their account, it will be deactivated. This seems to be the extent of the reprimand, which to the Intel unit would be a risk worth taking as the payoff of the information gathered would outweigh the risk of an account being deactivated.

The use of false accounts in social media (for intelligence purposes), is against the different company's policies. However, this practise does not currently break any New Zealand laws.

Currently the MSD Acting Security Intelligence Manager accepts the risk of using fake profiles to hide the identity of the analyst. This is in line and consistent with other New Zealand Government Agencies who have a regulatory function.

Profile to be used

The Intel Unit will have one login to use within the team across all four platforms.

The login will be set up as a 'skeleton' profile; no profile picture will be used, no pages liked and any interaction with comments/likes will not happen. This will make sure the profile does not mislead anyone further than already necessary.

This profile is not to be given to non-Intel team staff for use.

Setting up a new social media account

When a new account needs to be set up, this will be done by a senior staff member (with approval from the Manager Organisational Security Intelligence). This is to avoid accounts being created and not recorded.

Process:
1. An email account is set up using one of the free online services, e.g. Gmail or Hotmail.

2. This will be based on a 'firstname.lastname@___.com' format. The fictitious name is not to resemble any staff member across MSD. A check should be done through Global to confirm this.

3. Accounts are then to be created through the main five social media platforms:
   -Facebook
   -Linked In
   -YouTube
   -Twitter
   -Instagram

All will have the same user name (if required and possible) and password. Every effort should be made to link the logins with the different platforms.

4. All the login/user information is to be stored in a central intel social media repository in EDRMS.

Registry of Accounts

The Intel Unit will keep a registry of social media accounts stored in EDRMS. When a new account is created, the email address, user name and passwords are stored in the registry.

If an account needs to be deactivated the account will be deleted across all platforms, and a new account will be created in its place. The deactivated account will not be deleted off the registry, rather just noted that it has been deactivated. This way, records of all historical accounts are kept.

Non-authorised access to an account

If an attempt has been made to unlawfully access the account (across any one of the platforms or through the email address) that are on the registry, the email and account is to be deactivated. This is a safeguard measure, so historical searches and people cannot be identified or contacted.

The deactivation process will be undertaken by a senior member of staff and will be noted in the registry.

Process of collecting and storing captured online information

1. An analyst logs into the social media platform using the approved login.

2. They search for the person who is subject to investigation (verifying the identity as detailed below).

3. When the information needed has been identified, it is captured via SnagIt, and placed into a pdf document.

> -After each time an analyst has captured the relevant information, they are to put a statement at the end of the information captured stating the following:
>
> *"At the time of collection, all information was publicly available. Date: ____"*
>
> This is a safety measure showing the information was collected from a public profile, if it were ever questioned by the client.
>
> -All details such as names, pictures and comments made by anyone other than the subject must be removed from the captured information, or blurred out using the Snagit tool.

4. Once the intelligence product is complete, the report and attachments (including the captured social media data) are loaded into IMS and sent for investigation.

If a client submits an OIA/PA request, IMS notes and attachments are released, which will include the social media information that has been captured during the intelligence collection stage. Due to this, it has been identified that there is no need, at this stage to have a central repository to hold all social media data collected.

6(c)

Generic guides when searching for information

1. Only use the account that has been authorised.

2. Access the profile of the person in question the minimum number of times possible.

3. Do not interact with the person you are searching, i.e. friending them, commenting/liking posts.

4. Do not use social media platform to “fish” for other people and their details. All searched must be relatable back to the client/clients under investigation.

5. If information is captured from social media platform but the case is closed (no further action taken), the social media data must still be uploaded to the IMS case before it is closed off. This is to ensure that when/if a client makes an OIA/PA request, this information is accessible and able to be released. This information is also subject to the Public Records Act, which means that MSD cannot destroy the information it collects across social media.

Ministry of Social Development

Assessment of Information Gathering Process and Controls

28 September 2021

FINAL REPORT

Building a better working world

Contents

1. Executive summary

1.1 Background

The safe and appropriate use of information is an increasingly important challenge for government. Greater use of technology, the proliferation of information and analytical techniques, and better awareness of their risks, have led to a widespread debate over how to manage information in the modern world. Many organisations in New Zealand and across the globe are now contributing to better understanding of the legal and ethical implications of obtaining and using information, and this is a critical requirement for maintaining trust in the public service.

But the challenge for government's use of information goes beyond concerns about trust and privacy. Getting the right information in the right place at the right time is fundamental driver of value for money in government; making services work for the people who use them, improving government's systems and processes, and supporting better decision-making. The steps government needs to take to use information effectively are as much about good management, governance and planning within its existing activities, as they are about learning to work with disruptive technologies like Artificial Intelligence and Robotic Process Automation (RPA). The current focus on legal and ethical obligations of using information is as important opportunity for government to tackle these longstanding challenges in how it manages information right across government.

The Ministry of Social Development (the "Ministry") obtains a wide range of information in order to carry out its accountabilities. This information falls into two broad categories[1], these being; information necessary to deliver functions and services and information needed to give effect to the responsibilities agencies have to protect people, information, and places, to ensure regulatory compliance, and to detect and prevent criminal offending. Within the Ministry a key team involved in gathering information is the Intelligence Unit. This team enables the development of information about current and emerging fraud risk to inform the Ministry's approach to benefit fraud and to inform the Ministry's fraud work programme. Much of the information obtained and shared (internally and with other agencies) by Intelligence Unit is highly sensitive personal information about the Ministry s clients.

The Ministry's information gathering powers stem from the Social Security Act 2018 and the Public and Community Housing Management Act 1992. These Acts give the Ministry far reaching powers for obtaining information, which is critical for the effective administration of both Acts. These powers extend to the Ministry issuing notices requiring peop e to produce information and documentation. To ensure the Ministry is appropriately using these powers, Code(s) of Conduct[2] are issued to govern their use in practice. The Code(s) provide safeguards to protect an individual's right to privacy and ensure fair procedures are followed by the Ministry. These safeguards include a requirement the Ministry first seek information from a client before requiring the production of that information by a third party, unless to do so would prejudice the maintenance of the law

The 2019 Inquiry into the Ministry of Social Development's Exercise of Section 11 (Social Security Act 1964) and Compliance with the Code of Conduct revealed some weaknesses in how the Ministry exercised its information gathering powers, as some arrangements were inconsistent with its legal requirements, including the Privacy Act 1993. The issues identified resulted in infringements on individual privacy. On 1 December 2020 the new Privacy Act took effect. This Privacy Act introduces a new privacy principle (principle 12) and adjusts previously existing principles. Specifically, changes to Principle 6 introduce new refusal grounds that agencies, such as the Ministry, can use when responding to access requests.

Against this backdrop, the Ministry asked EY to consider whether the processes and controls the Ministry has in place to manage information gathering activities of the Intelligence Unit are designed and operating effectively. As the Ministry is dealing with sensitive client information, it needs to assure itself that arrangements in place to manage information gathering activities effectively mitigate the risk of gathering information to an acceptable level, i.e. processes are clearly defined and followed, and information is appropriately managed.

[1] Per the Te Kawa Mataaho model standards on Information Gathering and Public Trust

[2] Codes of conduct are accessible via the Ministry's website (www.msd.govt.nz).

1.2 Report structure and content

This report is prepared consistent with the AoG Consultancy Services Order dated 6 May 2021. It examines whether the processes and controls, that are used by the Intelligence Unit to manage information gathering activities are appropriate. The report addresses this question in two separate sections:

- Section One (the Executive Summary) summarises the work we have completed including our key findings and recommendations for the Ministry to consider.
- Section Two (the Assessment of Information Gathering Activities) examines the Ministry's information gathering processes and controls.

Our report draws on fieldwork completed in May and June 2021. Consideration was given to the external review completed over the Integrity and Debt Services operating model and the resulting re-design of the future state target operating model. Documents provided by the Intelligence Unit were reviewed in conjunction with interviews with key stakeholders. External reports, such as those completed by the Privacy Commissioner, were also considered.

Please refer to Appendix A for details of the objectives, scope, and the work performed. Stakeholders interviewed and documents reviewed are provided in Appendices B and C respectively.

1.3 General comment

We have assessed the maturity of the Intelligence Unit's information gathering practices to be at a "established[3]" level of maturity. The key controls and activities we would expect to be in place were evident but there is some variability in how these are applied in practice. In summary:

- Following the 2019 inquiry into the Ministry's exercise of Section 11 and compliance with the Code(s) of Conduct, there has been a greater focus on information and privacy risk management, which has led to improved practice in recent years.
- Work is underway to consider, and where deemed appropriate, implementation of the future state operating model for Integrity and Debt Services. This work is seen, by Integrity and Debt Services as critical step in ensuring the Ministry is positioned to ensure vulnerable New Zealanders are paid their correct entitlement, in full and in a timely manner. Importantly, this work will help shift the Ministry closer towards a more preventative model for integrity and fraud related services.
- Many features of a robust information gathering control environment are in place. For example, the Intelligence Unit has defined and documented how work is divided and done. This includes a rigorous quality assurance process to help mitigate the risks involved with the collection of sensitive personal information pertaining to the Ministry's clients. Notwithstanding this, we observed many of the Intelligence Unit's process documents (as included within the Intelligence Handbook) are outdated and are at varying degrees of maturity. The lack of up-to-date and comprehensively documented processes opens the Ministry to the risk that information gathering practices don't align to current practice or the Ministry's legal and ethical obligations. As an example, the Intelligence Unit's social media guidelines have not been reviewed since they were released in early 2017.
- During the course of our review we were informed that the Intelligence Unit uses pseudo social media profiles to gather information on clients. While the use of pseudo profiles is not uncommon in government, there is a need for increased scrutiny to ensure legal and ethical obligations are being met on an ongoing basis. This includes the obligations the Ministry has to adhere to the terms and conditions of the various social media platforms used by the Ministry. Following a Parliamentary Question in June 2021 the practice of using pseudo social media profiles was immediately suspended by the Intelligence Unit. In addition, a review and update of the Intelligence Unit's social media guidelines has been initiated. Communications with other agencies have also begun with the view to organising an inter-agency working group on the use of social media in intelligence activities.

At an "established" level of maturity further work is needed to ensure risks inherent to the Ministry's information gathering activities are being managed to more acceptable levels.

Cognisant of the improvements already being considered by the Ministry, the specific recommendations in the respect of our observations have been designed to supplement the activities which have already been undertaken/are in planning by the Intelligence Unit. Specifically, they are not designed to materially

[3] Refer Appendix D for a definition of the five-point rating scale we have used to assess maturity in the development of this report.

increase maturity to levels which are either undesirable or will take years and significant funding to implement but rather are designed to move the Ministry further along the maturity scale.

1.4 Key observations

Our key observations are summarised as follows:

Governance and oversight of information gathering activities

- **We observed a positive culture within the Intelligence Unit.** As previously noted, the information and privacy risk management culture within the Ministry has improved over recent years. Importantly, all interviewees within the Intelligence Unit demonstrated a strong commitment to their mahi, and ensuring they act in manner that is consistent with the Ministry's legal and ethical obligations (for example, ensure the sensitive personal information of Ministry clients is protected).
- **The Intelligence Unit have a strong Quality Assurance ("QA") process that includes two levels of review.** An initial QA is completed by the Principal Intelligence Analyst ("PA") which is followed by secondary QA by the Senior Intelligence Analyst ("SA"). Each have a slightly varied focus to ensure that all parts of the QA process are followed. The success of the QA process is also underpinned by the culture within the unit. The PA and SA make a point to know the Intelligence Analysts ("IA") well and understand their individual strengths and weaknesses.
- **Intelligence Officers have access to formal training.** The Ministry has provided formal training over the information gathering practices as governed by Schedule 6. These trainings are to be ongoing and are organised by the Capability Developer who sits within FIS. Training is supplemented by an informal mentoring program which provides Intelligence Officers access to ongoing guidance and advice. Additionally, there are fortnightly meetings to discuss issues that arise in the process of information gathering practices which ensures there is consistency in understanding and processes followed.

Design and establishment of information gathering processes and controls

- **How mahi is divided and done is defined and documented.** The Intelligence Unit have a 'Handbook' which acts as a central repository for all key process documentation. This handbook has is maintained by the SA and is used to guide and direct work. It is also used to onboard and train new team members from time to time. Notwithstanding this, many of the processes and practices documented in the Handbook are outdated and are at varying degrees of quality. The lack of up-to-date and comprehensively documented processes opens the Ministry to the risk that information gathering practices don't align to current practice or the Ministry's legal and ethical obligations. As an example, the Intelligence Unit's social media guidelines have not been reviewed since they were released in early 2017.
- **For the most part, controls supporting the information gathering practices of the Intelligence Unit are robust and operating effectively.** Through observation of information gathering practices, it was noted that the key controls we would expect to be in place are in place. This includes controls that restrict/limited access to information pertaining to clients and associated intelligence products. It is worth acknowledging that the majority of information obtained by the Intelligence Unit is from internal sources.
- **Document management and archiving practices should be strengthened.** While the Intelligence Unit have established document management and archiving practices for its cases, there is no guidance (for example, frequency of review) pertaining to the maintenance of the Intelligence Unit's processes. This creates a risk that the information gathering practices of the Ministry are not aligned with current practice, governing legislation and regulations, or recommendations of the Commissioner's Inquiry[4].
- **The use of pseudo or skeleton social media profiles is of particular concern.** The 'Interim Social Media Use Guidelines' were created in March 2017 and have not been reviewed or updated since. This document details the process of searching for publicly available information on social media platforms through the use of a skeleton profile. Current practice dictates this profile has no picture, no pages linked, and requires a fake name and email address to be set up. While the information gathered by these means is open source, the use of pseudo profiles can be viewed as deceptive and underhanded. It can also be seen as a breach of the terms and conditions of various social media platforms. It is

[4] Ministry of Social Development's Exercise of Section 11 (Social Security Act 1964) and Compliance with the Code of Conduct.

worth noting the Intelligence Unit immediately ceased use of pseudo social media profiles following a Parliamentary Question.

- **It is the view of the Intelligence Unit that IMS does not appropriately support end-to-end case management.** As such, the Intelligence Unit have developed the Work on Hand Tool ("CaseTool") for the purpose of reporting, tracking, and triage of cases. This provides visibility of work being done within the Intelligence Unit.
- **Additional information and guidance is required in relation to the application of security classifications and the processes that should be followed to ensure the integrity of information.** Security classifications and the differentiation between ratings were inconsistently understood by those interviewed and it is not clear how they are applied on a day-to-day basis.

Performance of information gathering processes and controls

- **Within the sample of 25 cases tested, 1 case deviated from expected practice**. This exception is of particular concern in that information was gathered on individuals not directly subject to investigation. We also noted that information required to be redacted (e.g., faces, names, comments, etc) were still visible in the documents reviewed. Please refer to Appendix G for further details on this exception.
- 9(2)(g)(i) [redacted] 9(2)(g)(i) This may include exploring opportunities the use of Schedule 6.1 to gather information on clients.
- **Specific controls could not be observed during sample testing**. We were unable to observe the existence of Risk Review and Quality Assurance practices within our sample as they are not tracked in IMS. However, we were able to gain comfort over the effectiveness of these controls through review of documented processes and practices, interviews and walkthroughs with stakeholders, and factors within the sample that indirectly indicated these processes had occurred. Please refer to Appendix G for details over cases where certain controls were unable to be validated.

1.5 Key recommendations

With reference to the above observations, we recommend that the Ministry consider the following key actions:

- **Complete the implementation of the future state operating model as it relates to the Intelligence Unit, and resource accordingly.** We are supportive of the direction the future state operating model for Integrity and Debt Services is taking in relation to the Intelligence Unit, in particular, recommendations to; create additional capacity for an Insights & Analytics capability, provide technical oversight, professional development, and coaching to the intelligence team, to implement and leverage advanced analytic techniques, and to transition from a responsive model to a prevention focused model. In the drive toward preventative intelligence gathering activities, standing up the future operating model is a critical step.
- **Review and update information gathering processes and practices.** The Intelligence Unit should conduct a full review of processes and practices that guide and direct its information gathering activities. Documented processes and practices should align with and support the implementation of the future operating model. This includes documenting processes and practices over information gathering practices that do not fit into the traditional mould of an intelligence case. For example, 'catch-and-pass' cases or cases owned by FIS in the first instance.
- **Complete the investigation into pseudo social media profiles and obtain a legal opinion on using social media as a source of information.** Guidelines over creation and use of social media accounts must align to the Ministry's current policy, and regulations applicable to the public sector. Legal

counsel over the use of social media will ensure privacy risks are effectively mitigated to an acceptable level. A full review of the practices for gathering information from social media must also be considered.

- **Establish robust document control mechanisms, including processes to independently review information gathering practices that could compromise public trust.** The Intelligence Unit should consider implementing a regular review and update of documented processes and practices. Current practice and regulation are always evolving. Documented practices should evolve in line with changes to the legal environment. Processes and practices must also align with the risk appetite of the Ministry and therefore changes to high risk information gathering practices should be independently reviewed.
- **Ensure there is shared understanding of how risks inherent to the Ministry's information gathering activities are managed to acceptable levels.** A shift toward the new operating model will bring new risks for the Ministry, especially in terms of client privacy with the introduction of more prevention focused activities. Changes to the activities within the Intelligence Unit need to include conversations with wider units of the Ministry to ensure the risks involved are appropriately mitigated. This includes the design and implementation of processes and practices that govern these activities.
- **Adopt a risk-based approach to reviewing and approving intelligence products.** The Intelligence Unit should prioritise QA of products based on the level of risk associated. Having two in-depth QA reviews is not necessary for all the intelligence cases. Detailed QA by multiple levels should be reserved for activities where there is a higher level of judgment needed or complexity involved.
- **Investigate where improvements can be made to exiting systems and tools.** The tools available to the Intelligence Unit, namely IMS, Objective, and CaseTool, are disaggregated and, in their view, fail to adequately support the wider activities that are performed. If this view is shared with Fraud Integrity Services and Internal Integrity, consideration should be given to identifying opportunities to implement tools that support the end to end case management, especially the more complex activities that will follow the implementation of the new operating model design. Any changes will need to be considered in conjunction with the Ministry's wider change portfolio.
- **Shift to using Objective for archiving cases and relevant artefacts**. Objective provides a platform for effective archiving of personal sensitive information gathered by the Intelligence Unit. However, many within the Intelligence Unit continue to use the E:drive to store cases and related sensitive personal information that has been gathered. It is recommended that the Intelligence Unit shift to using Objective for holding and archiving intelligence cases. Using objective to archive intelligence cases would ensure the Intelligence Unit's information management processes align with those of the wider Ministry.

Out of scope

[redacted] Limited
Out of scope
Partner - Consulting

Restrictions on the use of this report

Inherent Limitations

In the performance of our work we have undertaken tests of selected controls and transactions as appropriate to the circumstances of our review. The concept of selective testing, which involves judgement regarding both the number of transactions to be audited and the controls to be tested, has been generally accepted as a valid and sufficient basis for an auditor to express a view on the internal controls in operation. Occasions may arise where the nature of the controls, the lack of controls, or the circumstances of the review require us to undertake alternative audit procedures. The decision to test, or not to test controls is made by us solely at our discretion.

Because of the inherent limitations in any system of internal control or accounting system, errors, fraud or irregularities may occur and not be detected. The nature and size of the operations may prevent optimum segregation of duties being achieved. In addition, projections of any assessments provided on internal control relating to future periods (beyond the date of the audit fieldwork) are subject to the risk that the internal controls may become inadequate due to changes in conditions, or that the level of compliance with control procedures may deteriorate or weaken.

Our fieldwork was completed in July 2021. Our findings are expressed as at that date. We have no responsibility to update this report for events or circumstances occurring after that date.

Third party reliance

This report has been prepared at the request of the Ministry in connection with our AoG Consultancy Services Order dated 6th May 2021. This report is solely for the benefit of the Ministry for the purpose set out in this report, and is not to be used for any other purpose or distributed to any other party or relied upon by any other party without Ernst & Young Limited's prior written consent.

Other than our responsibility to the Board and Management of the Ministry neither Ernst & Young Limited nor any officer or employee of Ernst & Young Limited undertakes any responsibility or liability arising in any way to any third party, including but not limited to the Ministry's external auditor, in respect of this report.

2. Assessment of information gathering practices

This part of the report examines the information gathering processes and controls within the Intelligence Unit.

2.1 Overview of the Ministry's Intelligence Unit and its information gathering activities

Within the Ministry, a key team involved in gathering information is the Intelligence Unit. This team enables the development of information about current and emerging fraud risk to inform the Ministry's approach to benefit fraud and to inform the Ministry's fraud work programme. Much of the information obtained and shared (internally and with other agencies) by Intelligence Unit is highly sensitive personal information about clients.

There are three broad categories of work that occur within the Intelligence Unit; strategic, tactical, and operational. The allegations and referrals that are received fall under the tactical and operational areas of the Intelligence Unit. The cases that the Intelligence Unit gather information for form the basis of investigations conducted by Fraud Intervention Services ("FIS"). Everything that comes into and is released by the Intelligence Unit is over seen by the SA.

In 2020, the Intelligence Unit completed 135 intelligence cases. This fell 17% compared to 2019 and 55% compared to 2018. This can also be compared to the volume of Requests for Information ("RFIs") completed by the Intelligence Unit in 2020 which was 337. Despite the smaller number of cases completed by the Intelligence Unit, information gathering practices for intelligence cases forms a significant majority of their mahi.

2.2 Information gathering processes and controls

There are many risks associated with information gathering including but not limited to privacy breaches leading to a loss of public trust. The Government and the public expect the risks associated with information gathering practices to be managed in a manner consistent with its legal and ethical obligations.

Please refer to Appendix D for further description of the processes and controls over information gathering practices within the Intelligence Unit.

Ref	Expectation as determined by EY and with reference to our scope	High-level summary of relevant practices observed within provided documentation
1	The Ministry has established mechanisms (for example, accountabilities, key performance indicators and reporting structures) to govern and oversee the information gathering activities of the Intelligence Unit.	▶ There is a clear reporting structure within the Intelligence Unit and all information gathering activities receive two levels of QA. First by the PA and then by the SA. ▶ The development of a Target Operating Model ("TOM") in 2020 included a deep dive into the Intelligence Unit. The recommendations within the TOM include mechanisms to improve the governance and oversight of information gathering activities. The implementation of this TOM would lift already established mechanisms and create new ones to effectively mitigate the risks inherent in information gathering activities. ▶ The Fraud Referrals and Investigation Allocation Business Process outlines a clear escalation process within the Intelligence Unit. Risk escalation factors include cases where there could be reputational risk to the Ministry,

		involvement of gangs or organised crime groups, public safety concerns, staff safety concerns, among other things. Consideration is also given to the definition of high-risk cases which may include those that involve identity fraud, a previously unseen modus operandi, a system, policy, or procedural loophole, among other things. ▶ Where risk escalation factors or high-risk cases are identified, cases are able to be escalated within the Ministry based on the significance of the risk. The business process document also stipulates the roles and responsibilities at each level within the information gathering processes. This document has not been updated since 2015. ▶ There is an expectation that an Information Collection Plan ("ICP") is used by analysts in complex, high risk cases. To avoid confusion with ICPs completed by FIS the Intelligence Units ICPs are recorded in the case folder and archived in the E:drive.
2	The Ministry has established appropriate policies for the information gathering practices of the Intelligence Unit. These are designed to ensure compliance with relevant laws and regulations.	▶ The Ministry Ethics Framework contributes to the protection of the integrity of Ministry activities by providing ethical principles that underpin the Code of Conduct for obtaining information. The framework guides decisions made within the Intelligence Unit to ensure they are lawful, ethical, effective, and maintain public trust and confidence. ▶ There are multiple Codes of Conduct that govern the information gathering practices of the Intelligence Unit to ensure powers are used correctly. The Ministry Code of Conduct provides guiding principles over how the Ministry can collect, store, share, and use information and the impact on public trust. It also provides guidance over disciplinary actions when information is misused. ▶ There is also a specific code that governs how the Intelligence Unit obtains information under Schedule 6 of the Social Security Act 2018. The Code sets out the Ministry's information gathering powers under Schedule 6 and the relevant privacy considerations. ▶ Document control within the Intelligence Unit is not effective at ensuring documented processes and practices are up to date with current regulations. Having no regular review and update of information gathering practices creates a risk

		that current practices do not allow for compliance with relevant laws and regulation. ▶ A key example where processes and practices are not designed to ensure compliance with relevant regulations sits within the social media guidelines. The Interim Social Media Use Guidelines were created in March of 2017 and have not been reviewed or updated since. This does not reflect the 'Model standards for information gathering associated with regulatory compliance, law enforcement, and security functions'[5]. These model standards came into effect in December of 2018 and provide new methodology and regulation governing information gathering practices. The Intelligence Unit's use of social media for gathering open source information does not adhere to this change in model standards.
3	The Ministry has defined and documented appropriate processes and controls (for example, controls that help ensure the appropriate collection and use of information) to guide and direct the way information gathering activities are divided and done.	▶ The Intelligence Unit has specific processes and controls for different types of information gathering documented within their 'Intel Handbook'. This includes business processes for voice recordings, social media guidelines, Schedule 6 notices, data matches, data mining, information sweeps, among others. There are also process documents for Fraud Referral and Investigation allocation Business Process that guides the overall information gathering process. Notwithstanding this, we observed that many of the Intelligence Unit's process documents are out of date and at varying degrees of maturity. ▶ User access controls have been established to ensure the protection of any sensitive personal information gathered by the Intelligence Unit. ▶ A verification process controls the collection of sensitive personal information by ensuring the correct client has been identified in the Ministry's systems before any personal information is collected. ▶ Risk screening and risk escalation processes help to guide and direct the gathering of information by ensuring high risk cases have the appropriate oversight. The Intelligence Unit will not gather information on clients connected to high risk investigations without the appropriate approval and oversight within the Ministry.

[5] Acting in the Spirit of Service: Information Gathering and Public Trust (2018). States Services Commission SSC-Model-Standards-information-gathering-and-public-trust_0.pdf (publicservice.govt.nz)

		▶ Document control does not act as an effective control over information gathering practices. The lack of a formal document register and regular review of documented processes diminishes the ability to effectively guide and direct information gathering activities. This elevates the risk that processes, and controls are not designed to reflect current practice or relevant legislation.
4	The Ministry has training in place for employees making them aware of the importance of and their responsibilities with regards to privacy and protection of data.	▶ The Intelligence Unit provides all new staff with a desk file often referred to as the 'Intelligence Unit Handbook'. Documents included in this desk file detail the importance of privacy and protection of data. ▶ The information and privacy risk management culture has improved over recent years within the Intelligence Unit. Interviews revealed a commitment to the protection of privacy and acting in a manner that is consistent with legal and ethical obligations. ▶ Official training was provided to the Intelligence Unit when Schedule 6 was introduced as a governing power over information gathering activities. This training was organised by FIS and is expected to be ongoing. Additionally, fortnightly meetings are held where employees can discuss issues that arise within intelligence gathering activities. This allows the opportunity for issues to be solved and creates a greater level of consistency in work completed with regard to privacy and protection of data. ▶ 9(2)(g)(i) [redacted] This is seen to impact the Intelligence Units ability to get high risk cases transferred to FIS in a timely manner. As a consequence, the Intelligence Unit is less likely to use a Schedule 6 notice to obtain information due to the effort involved and the likelihood that information may be outdated once it is eventually received. This was confirmed in our sample testing where only 1 of the 25 randomly selected cases contained the use of Schedule 6 by the Intelligence Unit (4% of the sample). 6(c) [redacted]

		6(c) [redacted]
5	The Ministry has established appropriate tools and technology to support and enhance information gathering activities.	▶ The Intelligence Unit have created written scripts to extract data from Ministry source systems. The Data Scientists within the unit have built statistical models for early detection and data mining. Their ability to gather information internally is enhanced by the Data Scientists and other employees who have in-depth knowledge and skills required to perform data sweeps over the central Ministry database. ▶ The IMS tool is used to support information gathering activities by keeping records of intelligence cases and the information gathered throughout this process. However, the view exists that the tool lacks the appropriate functionality to effectively support the end to end activities of the Intelligence Unit or support enhanced information gathering activities. ▶ CaseTool is a platform created by the Intelligence Unit that acts as a work-around to provide additional functionality that does not exist in IMS to help support activities. However, there is a disconnectedness that arises from the lack of an appropriate tool to support end to end information gathering activities. ▶ Objective (formerly, EDRMS) is a central document repository that is available to the Intelligence Unit to store information gathered through intelligence activities. However, most intelligence analyst archive cases, and associated attachments, on the E:drive rather than Objective. Locations where cases are stored have access restricted exclusively to employees within the Intelligence Unit. Interviews revealed a desire to shift the archiving of cases from E:drive to Objective. Using objective to archive intelligence cases would ensure the Intelligence Unit's information management processes align with those of the wider Ministry.
6	Mechanisms are in place to monitor compliance with established processes and practices. The consequence of non-compliance is communicated to relevant stakeholders including employees so that they clearly understand the impact.	▶ The Intelligence Unit have a rigorous quality assurance process. All of the information gathered by the intelligence analysts is subject to two levels of QA. The initial QA is completed by the PA and the secondary QA is completed by the SA. This QA process ensures the information gathered is compliant with relevant processes and practices. Non-compliance with established processes and practices is not tolerated by the PA and SA.

		▶ As the Intelligence Unit is small in size, any non-compliance or general deviation from processes and practices and rectification is communicated directly with the IA. The PA attempts to gain an understanding of the individual strengths and weaknesses of each IA to ensure that any deviations are discovered and addressed. ▶ Despite the rigorous QA practices, a deviation from documented processes and practices was identified through sample testing. This was in relation to gathering of open source information. More detail on the exception identified is found in appendix G. ▶ The lack of effective document control processes does not lend itself to the effective monitoring of compliance with established processes and practices. If documented processes do not reflect current practices and relevant legislation, then any monitoring of compliance will be in vain.
7	Proper supporting records should be retained for the information gathering activities of the Intelligence Unit.	▶ The IMS tool provides a platform for the Intelligence Unit to retain supporting information for intelligence activities performed. However, the view exists that it does not provide adequate functionality to support the end to end processes of information gathering activities. Specifically, IMS does not provide a platform to support triage, tracking, reporting, or QA activities performed over intelligence activities. ▶ Intelligence products and supporting attachments are archived to allow the retention and maintenance of supporting records for the appropriate time period as dictated by legislation. However, Intelligence Unit process documentation provides inconsistent advice on the appropriate location to archive cases and supporting documentation. The Fraud Referrals and Investigation Allocation Business Process stipulates that supporting records are kept in Objective for all cases. However, the Case Administration for Analysts process map dictates that cases and supporting evidence are stored in the E:drive.

2.3 Managing information privacy risks

Information privacy is a key risk facing the Ministry when considering information gathering practices. The Government and the public expect information gathering practices to be carefully controlled to effectively mitigate privacy risks.

In 2019, the Privacy Commissioner completed an inquiry into the Ministry's information gathering powers under Section 11 of the Social Security Act 1964 and compliance with the Code of Conduct. It was found that information gathering practices were inconsistent with legal requirements and therefore an infringement on individual privacy. On 1 December 2020, the new Privacy Act took effect which introduced new refusal grounds for agencies when responding to access requests. Additionally, the introduction of Schedule 6 of the Social Security Act 2018 redefined the powers of the Ministry with regard to collecting sensitive personal information from other agencies.

Within our testing, the use of a Schedule 6 notice for gathering information was only captured once (4% of the sample). We noted no issues or deviations within this case. The Schedule 6 notices was observed to be in line with the Code of Conduct governing use of Schedule 6 and the business process used by FIS.

Ref	Expectation as determined by EY and with reference to our scope	High-level summary of relevant practices observed within provided documentation
1	The Ministry has processes and controls in place to manage privacy risks appropriately.	▶ The Ministry Ethics Framework acts as a control to align execution of information gathering activities to governing legislation and regulation. The ethical principles underpin the Code of Conduct and ensure privacy risks are effectively mitigated to an acceptable level. ▶ Both the Ministry Code of Conduct and the Schedule 6 Code of Conduct provide guiding principles over information gathering activities. These principles ensure privacy risks are considered and controlled at each point in the information gathering process. ▶ User access restrictions act as a control to effectively mitigate privacy risks over information gathered. Sensitive personal information that forms the basis of cases for investigation is restricted to the access of the Intelligence Unit employees. ▶ The use of Schedule 6 of the Social Security Act 2018 acts as a control to effectively mitigate privacy risks associated with information gathering from external sources to an acceptable level. Sensitive personal information can only be gathered from external sources through a Schedule 6 notice 9(2)(g)(i) This control was observed to be designed and operating effectively. ▶ Quality assurance processes act as a control to effectively manage the privacy risks associated with information gathering to an acceptable level. Two levels of QA are used to ensure information gathered follows documented

processes and practices to ensure privacy is maintained. QA also acts as an effective control over reputational risks to the Ministry. However, this stringent QA process is likely not necessary for cases with lower levels of risk.

- Regular review and update of documented processes and practices is a control that was not observed to be in place. The Intelligence Unit does not have a formal document register and does not regularly update documented processes and practices to reflect current practice or legislation. Document control does not effectively manage privacy risks appropriately.
- The controls surrounding the use of social media within the Intelligence Unit for gathering open source information are not designed and operating effectively.
- A control designed to manage privacy risks for use of social media is the blurring or redacting of information pertaining to individuals not subject to an investigation. This control is designed effectively but was not observed to be operating effectively. This process was not consistently applied as evidenced by the sample testing completed in the execution of this review. Please refer to Appendix G for further details on this exception.
- A control that would effectively manage the privacy risks associated with social media use to an acceptable level would be only searching for and capturing information over individuals subject to a case. The documented processes and practices around this point are unclear. The Social Media Guidelines state that 'pictures and comments must be taken from the person under investigation'. However, through interviews it was revealed that any information deemed relevant to the case can be captured, so long as a genuine need to collect information from social media is shown. 9(2)(g)(i)
- The ineffective controls within the Intelligence Unit over the use of social media for information gathering purposes not only poses an

		unmitigated privacy risk for the Ministry, but also a significant reputational risk.

Appendix A Objectives, scope, and work performed

Objectives

The objective of this engagement was to assess whether key business processes supporting information gathering practices by the Ministry's Intelligence Unit had appropriate controls to mitigate inherent process risks.

Scope

The scope of this engagement included:

- Information gathering activities undertaken by the Ministry's Intelligence Unit.
- Information managed and held by the Ministry's Intelligence Unit.
- The collection, use, and disclosure of personal information from / provided to other agencies (e.g., similar units in other government agencies).

The scope of this engagement did not include:

- Confirming compliance, or otherwise, with applicable laws and regulations that govern the Ministry's information sharing practices.
- Processes and controls outside of the Ministry's Intelligence Unit. This included processes and controls that are undertaken by other agencies.
- Assessing controls within supporting technology systems or infrastructure (other than considering restricted access to information).
- Verification of accuracy and completeness of information provided to EY.
- Anything not specifically identified as in scope in this engagement.

Work performed

Our approach to this engagement was as follows:

- Phase 1 - Plan: Involved undertaking meetings to mark inception of the engagement. The purpose of the meetings was to introduce our team establish communication protocols, discuss and reconfirm overall objectives and scope, and confirm our deliverables and timelines. In addition, the meetings served as a briefing session to detail the background of the Ministry's information gathering practices. Following this meeting, documentation was requested and examined to further our understanding of the Ministry's information gathering practices.
- Phase 2 - Deliver: Involved considering whether key business processes supporting the Ministry's information sharing practices had appropriate controls to mitigate inherent process risks.
    - Key process owners were met with to establish an understanding of the systems and processes related to the objective and scope was developed.
    - Document processes (where necessary) or validation of existing process documentation was conducted.
    - Key risks associated with these processes were identified.
    - Key controls to manage the risks and identify control gaps or overlaps were identified.
    - The effectiveness of key controls (i.e., do controls adequately address the risk and have they been operating throughout the period under review) were tested.
    - Fieldwork was collated, and the work performed was reviewed. The results were then summarised.
    - A closing meeting with the Ministry to discuss the preliminary results was conducted. These results were validated with the process owners as they were identified.
- Phase 3 - Report: In consultation with the Ministry, and using the insights gathered from previous phases, a draft, then final report was prepared for review and acceptance by the Ministry. The final report summarised the outputs of the engagement and clearly described our findings and recommendations.

Appendix B Stakeholder interviews

We would like to extend our gratitude to the following stakeholders for their time and insight.

#	Name	Position
1	Out of scope	Senior Intelligence Analyst
2		Principal Intelligence Analyst
3		Manager Intelligence Unit
4		Strategic Intelligence Advisor
5		Intelligence Analyst
6		Intelligence Analyst
7		Intelligence Analyst
8		Intelligence Analyst
9		Data Scientist
10		Operations Manager Fraud
11		Team Manager Information & Advice
12		Senior Advisor Integrity and Debt
13		National Manager Fraud Investigation Services

Appendix C Documents reviewed

#	Document Name
1	Privacy Commissioner Inquiry (2019)
2	Out of scope
3	Email - Background Information on Gathering (12 May 2021)
4	Out of scope
5	
6	
7	MSD Integrity and Debt (overview of the group and its functions)
8	Intelligence Unit Background
9	Privacy Act 2020 (From MAP)
10	Out of scope
11	
12	Organisational Security Intelligence Interim Social Media Use Guidelines (March 2017)
13	6(c)
14	Out of scope
15	Code of Conduct for Obtaining Information under Clause 2 of Schedule 6 of the Social Security Act (2018)
16	High Level Schedule 6 Process Flow for Fraud Intervention Services (2021)
17	Intelligence Unit - Fraud Referrals and Investigation Allocation Business Process (2015)
18	Context of Intelligence Unit
19	Mission Statement Intelligence Unit
20	Email - Section 11(e) Privacy Act (20 May 2020)
21	MSD Integrity Services Future Operating Model (2020)
22	MSD Integrity Insights and Intelligence Function - People Model (2021)
23	MSD Integrity Insights and Intelligence Function - Service Catalogue Process Design (2020)
24	MSD Ethics Framework
25	Schedule 6 Social Security Act (2018)
26	Email - Use of Privacy Act by the Intelligence Unit (25 May 2020)
27	Releasing Personal Information to Police and Law Enforcement Agencies: Guidance on Health and Safety and Maintenance of the Law Exceptions (2017)
28	Out of scope
29	
30	
31	

32	Out of scope
33	
34	
35	
36	
37	
38	
39	
40	MSD Intelligence Unit QA Template
41	Intelligence Unit Handbook pt.1 (2021)
42	Intelligence Unit Handbook - Data Mining
43	Intelligence Unit Handbook - Electronic Document & Records Management System (EDRMS)
44	Intelligence Unit Handbook - Security Response Programme Interim Health Safety and Security Assessment Process
45	Intelligence Unit Handbook - Peer Review Guidelines (2017)
46	Intelligence Unit Handbook - Suspicious Transaction Guideline (2013)
47	Intelligence Unit Handbook pt.7
48	Intelligence Unit Handbook - Fraud Intervention Services Model of Practice (2019)
49	Intelligence Unit Handbook - IMS Resource Book
50	Intelligence Unit Handbook - IMS Changes (2019)
51	Intelligence Unit Handbook - Privacy Commissioner A Quick Tour of the Privacy Principles (2016)
52	Intelligence Unit Handbook - Code of Conduct (2011)
53	Intelligence Unit Handbook - Help Happening How we Support Fraud Teams (2016)
54	Out of scope
55	MSD Intel 'Sweeps'
56	MSD IRD Information Sharing Agreement (2018)
57	MOU Between MSD & IRD for the Supplying of Information to Assist the MSD to Reduce Benefit and Subsidy Overpayments (2018)
58	MOU Between MSD and IRD for the Supply of Information for Working for Families Tax Credits Administration (2018)
59	MOU Between MSD and IR for Working for Families Tax Credit and Benefit Double Payment (2018)
60	MOU Between MSD and IR - Limited Information Share for Updating Customer Contact Information (2018)
61	Acting in the Spirit of Service Information Gathering and Public Trust (2018)
62	Information gathering standards update (11/6/2021)

63	Out of scope
64	
65	

Appendix D Information gathering process overview – Allegations / fraud referrals

The Manager of the Intelligence Unit is ultimately responsible for all products of the Intelligence Unit. The SA and PA report to the Manager and are supported by a team of four IAs, a Strategic Intelligence Advisor ("SIA"), and a Data Scientist.

In the first instance, an allegation or referral is sent to the Intelligence Unit and received by the SA. The SA will perform preliminary analysis to allow the case to be triaged. This includes a screening and risk escalation completed by two senior staff within 48 hours. Where risk escalation factors are identified, the case will be escalated to the Director of Intelligence. The risk escalation factors are laid out in the fraud referrals business process and include the potential for media interest, involvement of public figures, reputational risk to the Ministry and child safety concerns, among other things. Consideration is also given to the definition of a high-risk case. High risk cases include those with a previously unseen modus operandi, those that are sophisticated, those with political or reputational risk, or those that involve organised crime, among other things.

The screening and risk escalation practices are not formally tracked in IMS or CaseTool.

In some instances, the initial analysis and risk review will reveal that no further action is required on the part of the Intelligence Unit. This may mean the case is stopped completely, transferred to the front line, transferred to FIS, or escalated to a higher level. If the initial screening and risk review presents information that warrants further information, the SA is able to prioritise cases. Cases deemed to be of high risk or including risk escalation factors will be assigned to the next available IA.

The IA takes on the case and performs the information gathering and analysis. The IA will determine whether fraudulent activity is present, and to what extent, using analysis over information gathered. 6(c)

6(c)

When using social media, the Intelligence Unit are deemed to be 'passive users' meaning they do not interact or engage with the subjects they are collecting information on. Only publicly available information is able to be collected and all information relating to those not subject to the investigation must be redacted or blurred. Our testing showed these guidelines to be applied inconsistently by Intel. Additionally, the Intelligence Unit must be able to show a genuine need to collect the information, either through an open investigation, a detailed Data Mining Project plan, or an imminent threat situation developing. It is unclear whether the Intelligence Unit are able to conduct social media searches and gather information on individuals not directly subject to investigation. Documented processes and practices suggest only capturing information over individuals directly subject to investigation. However, current practice suggests that information can be captured over those not subject to investigation, if there is a genuine need. However, this does appear to be unnecessarily invasive and a potential intrusion of privacy on the general public.

A desk-file, aptly named the 'Intel Handbook', contains all the relevant documents for the Intelligence Unit. This includes templates used for referrals and assessments and all of the guidelines around information gathering practices. This desk-file provides detailed resources for members of the Intelligence Unit for any process or activity they might undertake.

After they have gathered all information pertaining to the case, the IA will analyse the information. They use the information and analysis to make a decision over the progression of the case. Analysis may reveal no indication of fraud and therefore no further action required by the Intelligence Unit. Alternatively, fraud may be revealed, and the case can be forwarded on to FIS. The IA will determine, with support from the PA, whether a referral or a full assessment is appropriate for each individual case. A referral is a shorter report that outlines the key findings from the information gathering activities. An assessment contains a deeper level of information gathering and analysis that forms a more in-depth report. It provides a full picture to the FIS team.

Throughout the information gathering and analysis phase the IA will perform weekly risk assessments. The PA will assist the IA in decision making for the duration of the case. They will also conduct fortnightly risk assessments and audits of the information contained in IMS. At any point if the PA or IA identifies new risks that warrant further investigation the case can will be escalated appropriately. While these risk assessments and audits are conducted over the information contained in IMS, there is no tracking or indication of this process in IMS.

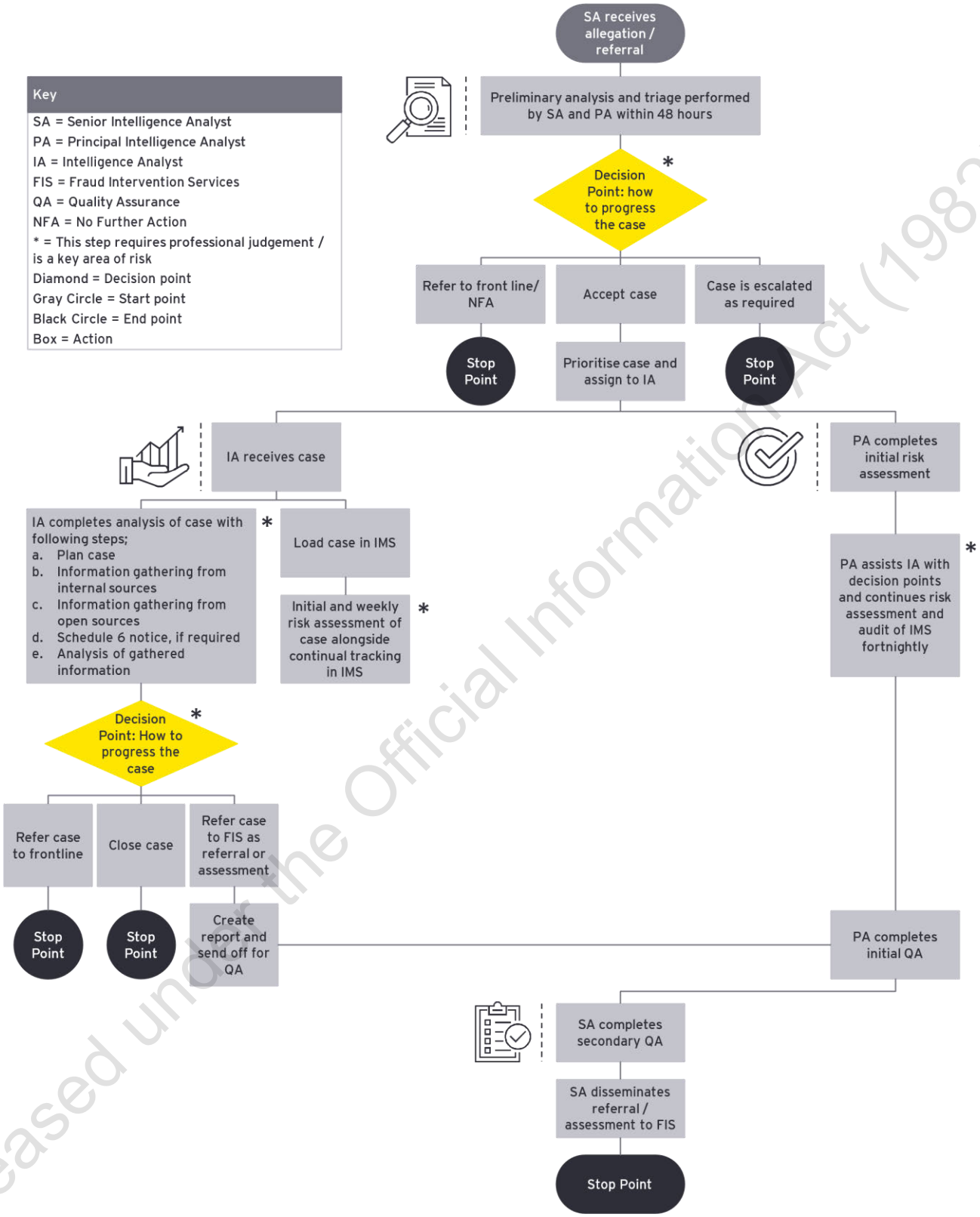
Once the case is completed, it will be handed off to the PA for initial QA. The PA does not use a formal QA template. The current PA has created their own general categories to inform the QA process. These include: Sources and Agencies, Collection, Analysis, and Challenging the Analysis. Within the analysis category the PA will look into the qualitative / quantitative analysis, hypothesis generation, analysis tools applied, assessment, and strategic analysis. They will also attempt to understand the structured thinking and strengths and weaknesses of each analyst to better inform this process. When challenging the analysis, the PA is trying to help the IA understand what they can do better and investigate any opportunities.

The PA will then hand off the case to the SA for secondary QA. The SA does follow a QA template which includes the categories of General, Findings, and Analysis. The secondary QA process is less detailed oriented than the initial QA and focuses on ensuring the product is ready for dissemination. As part of this QA process, both the SA and PA have made a point to get to know each of the IAs within the unit. They find by understand their style of work and thought process they can gain insight into the strengths and weaknesses of each IA. The QA process then becomes more personalised than a typical QA. Both the SA and PA are able to use this QA process to help guide and support their IAs to produce the highest quality products.

The two levels of QA act as a control to mitigate many of the risks within the information gathering process. The Intelligence Unit are ensuring that all products that are created follow appropriate processes and practices and adhere to any applicable legislation. While this effectively mitigates any risks for high profile or high-risk cases, it could potentially be excessive for lower risk cases.

While the Manager of the Intelligence Unit is ultimately responsible for all products created by the Intelligence Unit, it is the SA who actually disseminates the final product to the end user. This dissemination occurs in the IMS tool, but the SA will also email FIS to inform them that the case has been handed over.

Information regarding a case is stored in IMS and access to IMS is limited to those who need it. However, there is an inability to effectively track and report on cases from inception to completion within the IMS tool. Additionally, cases are archived either in Objective or the E:drive.



Appendix F Maturity rating definitions

EY's internal audit maturity model incorporates five levels along the maturity continuum, defined as:

#	Name	Description
1	Basic	Information gathering practices are not clearly defined or documented. The control environment within the Ministry is not designed or operating effectively. Mitigation of key risks over information gathering practices are rudimentary.
2	Developing	Basic documentation exists over the processes and practices for information gathering practices. The Intelligence Unit has plans for improvement of the control environment. The Intelligence Unit focuses on mitigation of compliance risks.
3	Established	The Intelligence Unit has clearly defined and documented processes and practices over information gathering practices. Documented processes and practices are reviewed and updated regularly to reflect current practice and relevant legislation. The control environment is generally robust and operating effectively. Risks over information gathering practices are, for the most part, mitigated to an acceptable level.
4	Advanced	Processes and practices governing information gathering practices are well defined and documented. Regular review and update occurs to ensure process over information gathering are designed to ensure compliance with relevant laws and regulations. The Ministry is proactive in its attempt to identify new and emerging risks. The control environment is robust, well designed, and operating effectively. Controls over information gathering practices effectively mitigate key risks to an acceptable level.
5	Leading	The processes and practices over information gathering practices provides an environment that encourages preventative intelligence activities. Information gathering practices are considered leading when benchmarked against a peer group. There is proactive continuous improvement of the control environment. New and emerging risks are continuously analysed and appropriately mitigated.

Appendix G Information Gathering Testing Exceptions

The following table identified instances where the process of information gathering followed deviates from documented processes and practices.

Case Reference	Explanation/Comment
95506	Information has been gathered via social media for individuals who are not subjects of the case. The Intelligence Unit believe this is justified as it provides evidence that the subject was not located in New Zealand and therefore relevant to the case. It adheres to showing a 'genuine need' to collect information from social media. However, this could be considered unnecessarily invasive and an intrusion of privacy. Especially if these individuals are not clients of the Ministry. The Intelligence Unit are required to blur out faces and information of individuals not relevant to the case when completing social media information gathering. This process was not consistently adhered to within this sample. As per documented social media guidelines, the Intelligence Unit are required to put a statement after each piece of information captured. This confirms that the information collected at this date / time was publicly available. This guideline was not consistently followed for this case. The SWN number of one of the subjects differs between IMS and internal information gathered. However, the reason for this is noted in IMS as being a stolen identity and therefore having two profiles with the Ministry.

The table below identifies instances where controls over information gathering practices were unable to be observed in our testing.

Case Reference	Explanation/Comment
91306	The intelligence product associated with this case was transferred to FIS for further investigation via email, and not uploaded to IMS. This means we were unable to validate the completion of certain QA processes for this case.
97055	This case was considered a 'catch and pass' meaning it was transferred to FIS via email after triage. This case was not loaded into IMS by the Intelligence Unit and we were unable to validate the completion of certain risk review and triage processes.

EY | Assurance | Tax | Transactions | Consulting

About EY

EY is a global leader in assurance, tax, transaction and consulting services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation is available via ey.com/privacy. For more information about our organization, please visit ey.com.

ey.com

Ministry of Social Development

External Fraud Information Gathering Policies and Processes
2022

1. Introduction

In late 2018 an Inquiry Report was delivered by the State Services Commissioner in response to concerns about the use of external security consultants by government agencies. Several agencies were identified in breach of the State Services Code of Conduct or had acted unlawfully. As a result, the State Services Commissioner issued Information Gathering and Public Trust Model Standards[1] (the Model Standards) setting minimum standards for information gathering associated with regulatory compliance, law enforcement and security functions. The Model Standards are effective from 18 December 2018.

In 2019 the State Services Commission asked Chief Executives of government agencies to report on their agency's compliance with the Model Standards. At the time of this request the Ministry was responding to the Privacy Commissioner's Inquiry into its use of statutory demands under section 11 of the Social Security Act 1964 (now Schedule 6 of the Social Security Act 2018). The State Services Commission agreed that the Ministry could defer reporting on several aspects of the Model Standards for the first-year review until it had managed the response to the Privacy Commissioner's Inquiry. The Ministry's response involved the review and reform of its external fraud information gathering policies and processes.

There is a strong correlation between the Model Standards and the recommendations that arose out of the Privacy Commissioner Inquiry. They both deal w th the collection of personal information from or about individuals in the context of compliance or law enforcement activities. Both set or reset standards that must be maintained when collecting information and in particular personal information, including in general terms that the activity is lawful, necessary, and proportionate to the purpose for the collection.

Simply Privacy is engaged to review the Ministry's implementation of the remaining Model Standards yet to be reviewed. In the light of the context of the State Service Commissioner's inquiry this review has focussed on the policies and processes used by Ministry to undertake its fraud investigations. We were aided in this review by our earlier review of the implementation of the Codes of Conduct for Obtaining Information under clause 2 of Schedule 6 of the Social Security Act 2018 (replacing Section 11 of the Social Security Act 1964) and section 125 of the Public and Community Housing Management Act 1992 (the Codes).

1.1 Review Requirements

The Ministry's response to the external fraud information gathering Model Standards and the Privacy Commissioner's recommendations were completed in early 2021 and included policy, guidance and systems changes, and the introduction of the Codes that regulate the way in which the Ministry uses statutory demands in their investigative work. The Codes came into force 1 March 2021.

In April 2022 the Ministry issued Terms of Reference[2] seeking assurance that the revised external fraud information gathering policies and processes are compliant with the Model Standards. In particular the review is to focus on the two Model Standards still to be reviewed,

- Legislative and Policy Framework
- The "Implementing Strong and Comprehensive Policies" part of the Organisational Safeguards section.

[1] The full title is "Information Gathering and Public Trust – Model Standards for information gathering associated with regulatory compliance, law enforcement and security functions – Effective from 18 December 2018".
[2] See Appendix 1

The model standards under review are set out in ***Appendix 2.***

The review is to assess fraud information gathering policies alignment with the Model Standards by,

- assessing the articulation of the model standards in the information gathering policies
- assessing if the information gathering processes effectively support policy implementation
- assessing any outputs of any ongoing compliance assurance activities for external fraud information gathering policies and processes
- testing a sample of relevant records to verify compliance with the Information gathering policies and processes.

We were provided with full access to the Investigation Management System (IMS) which holds digital records of investigation files. We were also given access to the Ministry's internal website, Doogle, which enabled access to policy and procedure documentation and advice.

We reviewed a substantial number of policy and guidance documents, and a total of 70 investigation files out of an estimated 1600 current and closed files. Many of the files were still under active investigation and involved complicated long running fraudulent behaviour. We reviewed an estimated 150 to 200 statutory demands. We had full access to a wide range of staff involved in the compliance and enforcement area.

2. Information Gathering Policies

Policy Specific to Information Gathering

The Ministry's policy and general guidance includes a broad range of advice about information gathering and related issues. The policies that were most relevant to the Model Standards are listed in Appendix 3. They reflect good practice and incorporate the expectations of the Model Standards, the applicable law and the Ministry's own Code of Conduct. They are cognisant of the rights and responsibilities contained in the Ministry's enabling legislation including the Social Security Act 2018 and the Public and Community Housing Management Act 1992 (together the "enabling legislations" for fraud investigations). In appropriate contexts the policies also reflect the New Zealand Bill of Rights Act 1990 right to be secure against unreasonable search or seizure, whether of the person, property, or correspondence. Similarly, the Search and Surveillance Act 2012 is highlighted for its obligations and restrictions on search of people and places.

The Privacy Act features strongly in all policies that set expectations around personal information management, gathering, and security. In combination with the expectations within the Model Standards and the specific requirements of the Codes the policies require staff to establish clear purposes for the collection of information. This includes demonstrating within work files the necessity, relevance, and proportionality of the required information. The privacy content is noticeably influenced by the recommendations and wider commentary made by the Privacy Commissioner in his inquiry into the use of statutory demands.

An example of the fulsome advice included in the Ministry's policy portfolio is contained in the "Investigation Process"[3] policy and guidance. The section is easily accessed on the Ministry's internal website. At an opening level it includes a focus on the key steps of,

[3] Investigation Process – August 2022

- analysis of information and data
- planning an investigation
- arranging interviews with clients and witnesses
- interviewing and taking statements
- considering a search warrant
- decision making
- the prosecution processes

These commentaries leverage to more specific advice including,

- Investigation techniques
- Gathering Information – Benefit and Housing Fraud
- Determining Clients Relationship Status
- Security of Information
- Evidence of Relationship Status
- Fraud Indictors
- Use of Dictaphones
- Requesting and Executing Search Warrants

The advice throughout these various documents is comprehensive and accommodates the information gathering expectations within the Model Standards. The policy is connected to good guidance about operational process for example the full and inclusive advice contained in the 'Gathering Information' document. This document has full step by step advice on the process for completing statutory demands with an accompanying very useful FAQ section. It explains the provisions of the Ministry's enabling legislations, and the requirements of the Codes including the need for transparency, necessity and proportionality when collecting information. There is a link to a high level process flow chart and clear instructions about managing information that is neither necessary or relevant. The guidance aligns with the Model Standards.

NZ Bill of Rights Act

We noted that there are references to the New Zealand Bill of Rights Act for example in the "Contractors and Consultants – April 2022" policy. It is a brief reference to the legislation being a special consideration. The Tāu Raurau training material covers section 21 rights to be secure against unreasonable search and seizure. Apart from those references we did not find broad commentary in policy or guidance to the relevance of the Bill of Rights or case law dealing with unreasonable search and seizure issues.

Recent case law[4] is particularly important to understanding obligations where requests for voluntary disclosure of information are made and where the disclosing agency is being asked to rely on Information Privacy Principle 11(1)(e) exceptions. The case raises the importance of the Privacy Act and its relationship with other relevant statutes, such as the Search and Surveillance Act 2012 and in particular the use of productions orders. It also highlights the test for the admissibility of evidence under section 30 of the Evidence Act 2006 and the test for an unreasonable search under section 21 of the New Zealand Bill of Rights Act 1990. These were important aspects of the Privacy Commissioners views in his inquiry report that dealt with a reasonable expectation of privacy and unlawful or unreasonable search. The focus of the Privacy Commissioner and courts was on protecting a biographical core of personal information which may include information which tends to reveal intimate details of the lifestyle and personal choices of an individual.

[4] *R v Alsford [2017] NZSC 42*

The policy "Police Reports on Person Under Investigation and Witnesses – March 2016" is an example of guidance where we would have expected reference to both section 21 of the NZ Bill of Rights and the Supreme Court decisions. Both of these legal considerations and the case law would be helpful considerations in the creation and service of the statutory demands and compliance with the Codes. They would also be influential in the application and use of clause 1 of Schedule 6 (Duty to answer questions asked by MSD).

Contractors and Consultants

The policy content includes two almost mirror policies that deal with the engagement of external consultants in general and services that include specialist investigations. One of the two policies[5] highlights External Security Consultants and includes special considerations that apply to them. While the policy has a main focus on procurement it adequately highlights the requirements of the Model Standards and imposes a special procurement process that includes approval by the DCE Organisational Assurance and Communication. The policy is backed up by a useful process document[6] that operationalises the procurement process.

Policies on Storage and Security

There is an adequate array of policies and guidance that sets standards around storage/security and destruction of data.

The Codes require analysis of received information and proactive redaction or destruction of information that is neither relevant nor proportionate to an investigation. A specific policy[7] requires all information to be saved to a Ministry approved information management system such as the Client Management System (CMS) or the Investigation Management System (IMS). These systems are automatically managed by the Ministry through business rules that dispose of information according to the requirements of the Public Records Act 2005.

Two related policies[8] deal with the general security of information and acknowledge the interdependence of information security and privacy. There is a strong reliance on the Information Privacy Principles in the Privacy Act 2020.

3. Information Gathering Processes

The Codes are influential on both the processes and practices of the Ministry's investigation teams. The Codes are shaped by the Ministry's enabling legislations, recommendations of the Privacy Commissioner, the Privacy Act's Information Privacy Principles, the principles of natural justice, and the current common law on search and the right to privacy. The synergies between the Codes and the Model Standards are acknowledged by the Ministry and are integral to the information gathering activities of investigators. These various obligations are appropriately reflected in information gathering guidance, the current processes adopted with the investigation teams, and training.

The regulatory compliance and law enforcement aspect of the Ministry's work is undertaken by the Investigations Teams. They include,

[5] Contractors and Consultants Policy – April 2022
[6] Use of External Security Consultants Process – June 2019
[7] Disposing of Information
[8] Information Security Policy; Privacy and Security of Information Policy.

- The Client Services Integrity (CSI) team, responsible for investigations into external fraud
- the Internal Integrity team responsible for fraud involving the Ministry's employees
- Client Support Debt Management, responsible for managing client debt and verifying plans to repay
- the Intelligence Unit.

All teams use approved information management systems with the enforcement work predominantly held in the Investigation Management System (IMS). This system is structured to hold all data relating to an investigation in a variety of tabs, drop down menus, free text areas and uploading document capabilities. In appropriate places information input is mandatory. The IMS is the first and predominant source of investigations information.

The recording of information requirements of the IMS are detailed and comprehensive and a digital investigation file includes,

- reports detailing the justification for gathering information
- justification for bypassing a client and going straight to a source for information
- approvals at appropriate senior management levels
- interactions with a client
  interactions with witnesses and informants
- interviews including audio files, transcripts, and written statements
- copies of a statutory demands
- descriptions and the content of information received, and
- management and analysis activities of information received for relevance, retention, or disposal.

The IMS is designed to accommodate the specific requirements of the Codes for gathering information under the enabling legislations In tandem with the writing of the Codes substantial changes were made to the IMS to accommodate the comprehensive expectations within the Codes.

Expected information gathering practice is set out in a thorough 53 page practice guide[9] which includes a useful flow chart, commentary about how information must be collected along with the details of justifications and approvals. Each advice area is accompanied by an "Action Required" note which describes the specific action required of both investigators and managers.

Investigations staff are fully informed by the policy and guidance and it is readily available to them. Managers are required to maintain active oversight of the investigations work to ensure that information gathering policy and guidance is adhered to by all staff. They operate within a defined 1st line of defence capacity. The managers are also integral to the approvals that are required at key steps in the information gathering cycle. In addition managers perform a training obligation for staff new to the role of an investigator.

Current training comprises three mandatory Tāu Raurau units:

- Two introductory privacy modules (Privacy ABC and Privacy Act 2020), from the Office of the Privacy Commissioner's e-learning framework.
- An in-house customised unit "A fresh look at our Ethics Framework and Codes of Conduct."

[9] Practice Guide – Investigation Information Gathering – August 2022

- A five-module unconscious bias programme, focused on diversity, inclusion, and understanding and addressing bias in the workplace

For new staff, the induction programme incorporates the three Tāu Raurau units, along with an in-person workshop that focuses on understanding and integrating the Codes into work routines. As mentioned above new staff also undergo initial supervision, in which 100% of their work outputs are reviewed by a manager or trainer until full competency is obtained in the process and expectations of the role.

4. Information Gathering Assurance

The assurance process and audit in place for the investigations activity including information gathering is comprehensive, active and effective. Aspects of it are completed in near real time and operational and internal strategic stakeholders are regularly informed about the issues that arise and the adequacy of controls to manage risks associated with information gathering. The introduction of assurance reviews around the Codes compliments the prior existing general targeted audits. In combination they focus on a total view of the investigations practices and outcomes. The streams of audit are wide-ranging and inclusive of the obligations in the Codes and the Model Standards.

Assurance Reviews

As a result of the Privacy Commissioner's Inquiry the Ministry established the Codes and a comprehensive assurance programme and process which commenced in 2020.This audit function is established along the "3 lines of defence" assurance reporting model. The 1st line activity within the Investigation Teams involves both managerial oversight and approvals, and regular checks by the embedded assurance advisers who monitor all investigations carried out in the Investigation Teams. The audit is carried out in near real time. Feedback is timely and regular.

A 2nd line assurance check is undertaken by a full-time dedicated staff member in the Information Group (IG) which operates and reports independently from the Investigations functions. The 2nd line assurance reviews are conducted monthly after statutory demands are served by the Investigation Teams.

Targeted Audits

The Codes audit process leverages off existing targeted audits of investigations which are also carried out by an Investigation Assurance Officer. These audits may result in reports to investigations staff and managers for remedial action. In the case of performance or development needs a case conference involving the investigator, manager and assurance adviser may be undertaken. These monthly audits target investigations according to what is occurring across the fraud workload and the focus is arrived at through input from fraud managers along with trends identified through prior audits, review decisions and complaints. The current targeted audits focus on consistency of operations across investigation teams and currently, the teams' tolerance for fraud. This requires a full end to end audit of an investigation file. The data collected will become part of a report for the Organisational Health Committee.

New Staff

As mentioned above, a further assurance and monitoring approach is adopted with staff who are under development, that is staff who are new to the work of the Investigation Teams. This process requires all managers to closely monitor the work of the new staff by undertaking regular reviews that are in real time and recorded. This review by the managers is continued until a staff member is considered competent in all aspects of investigative work, at which time

their file monitoring would be handed over to the 1st line assurance team for ongoing review as applied under the national assurance programme.

Overall

The audit system and process are detailed in guidance[10] and for the Codes, supported by a comprehensive audit and assurance plan[11]. The audits focus on general competence in investigations and the objectives include,

- All investigations are completed to a high standard
- Evidence supports decisions, is fully documented and supported by relevant legislation, policy and case law
- Legislation, policy and case law is correctly applied
- Evidential statements adhere to Ministry procedures
- Fraud work is conducted with integrity and professionalism in line with the Ethics Framework
- Risk is identified, documented and escalated at earliest opportunity
- All information handled in accordance with Ministry policy
- Privacy Principles are adhered to
- Investigators are developed to be fully competent

All audits involve the use of template reports, feedback to managers and investigators and where appropriate remediation actions for both the investigation and staff. Remediation activity is approved and closed out by managers. Summary reports are delivered monthly to senior governance boards[12] detailing the level of review, noting any issues identified and remediation steps put in place to improve practices.

On a monthly and quarterly basis the assurance advisers summarise their activities noting the trends in issues and detailing the remediation in individual files or system changes that were required to alter staff practice. These reports build an ongoing and contemporary narrative about the state of activity of information gathering in the investigation teams. The monthly reports are shared with managers and governance boards.

5. Conclusion

As a result of the publishing of the Model Standards, the recommendations of the Privacy Commissioner and the delivery of new Codes, the Ministry has undertaken a significant change to the way that information is collected, used, and managed in its investigations. The change has included reviewing existing policy and guidance, introducing new policy and guidance, and upgrading training. The processes and systems used by the investigations teams have been modified including significant changes to the IMS to establish requisite standards of recording information and actions. These changes are audit enabling. There is a healthy range of policy that deals with the gathering of information with a focus on the lifecycle of information from collection, through use to disposal. The policy is backed up with useful guidance, operational documents, and flow charts. The Model Standards while not always referred to explicitly in policy is clearly visible by analogy. We felt that there would be merit in an increased focus on the obligations contained in the NZ Bill of Rights Act, section 21, and the common law principles around the right to privacy contained in recent case law such as *R v Alsford.* [13]

[10] Client Services Integrity Services – Assurance Process – April 2022; 0
[11] Assurance Plan for Codes of Conduct – circa late 2020
[12] Client Integrity Management Board; Organisational Health Committee.
[13] Supra footnote 5

There is significant and detailed effort by the assurance advisers who review and record their work in a variety of templates and reports. Through our sampling of individual assurance case reports and summary reports it was demonstrated that the auditing is thorough, constant, and effective in highlighting issues and reducing risk in the task of information gathering. As might be expected of a new and developing system the audits showed that early on in deployment there were issues that needed correction and remediation. Over the year of work that we reviewed[14] there was a noticeable decline in the number of issues identified. It was evident that the assurance audits were influencing staff behaviour and establishing information gathering practices that are compliant with the Codes, the Model Standards, and the law.

Our review of fraud investigation files showed that there is significant workplace endeavour to absorb and comply with the Codes and Model Standards. It is apparent that staff and managers have a strong focus on ensuring that information gathering complies with the law, the Codes and policy. The combination of management oversight and assurance audits is contributing to a culture of demonstrating through reporting, the substantiation for information gathering activity, focusing on purpose, necessity, proportionality and relevance. The culture is also considerate of natural justice considerations that ensure clients are, at appropriate times, fully informed about the Ministry's investigations and that as clients, they may have control over the information about them.

Overall, we are confident that the Ministry has introduced policy, gu dance and processes that are aligned with the Model Standards. They have been readily adopted by staff and there has been significant changes to the way operational activity around gathering information is undertaken. There is a healthy culture and endeavour among staff to comply with law and policy around information gathering.

[14] March 2021 to March 2022

Appendix 1 – Terms of Reference for Review of External Fraud Information Gathering Policies and Processes

Terms of Reference

External Fraud Information Gathering Policies and Processes

Purpose

This review is intended to provide an independent and objective view on MSD's application of the Information Gathering and Public Trust model standard to external fraud information gathering policies and processes.

Context

In December 2018 the State Services Commission (now Te Kawa Mataaho Public Service Commission) released the Information Gathering and Public Trust model standard. This was in recognition of the need to provide a set of information gathering expectations to public sector agencies whose responsibilities, when exercising the power of the state, necessitated information collection. Agencies are expected to use the Information Gathering and Public Trust model standards when establishing or reviewing their information gathering policies and practices to help ensure they will act in accordance with their authority and in line with what the public generally expects and considers reasonable.

In 2019 the State Services Commission asked each Chief Executive to report on their agency's compliance with the model standards. At the time however, MSD was responding to the information gathering findings of the Office of the Privacy Commissioner's inquiry into MSD's use of Section 11 (Social Security Act 1964). The planned response included remediation work to address any gaps in MSD's external fraud information gathering policies and processes. The State Services Commission and the Ministry agreed the Chief Executive would delay reporting on the model standard implementation for external fraud information gathering until after the remediation work was complete.

The revised external fraud information gathering policies and processes have been operating for over a year. This review is designed to provide assurance that those policies and processes support the related expectations[1] of the Information Gathering and Public Trust model standard and are being operating effectively. Recommendations will be made to strengthen policies and processes if gaps or misalignment to the model standard are identified.

Timing for this review will be agreed with the sponsors.

What we will do

We will assess if the external fraud information gathering policies and processes give effect to the Information Gathering and Public Trust model standards by:

- assessing the articulation of the model standards in the information gathering policies
- assessing if the information gathering processes effectively support policy implementation
- assessing any outputs of any ongoing compliance assurance activities for external fraud information gathering polices and processes
- testing a sample of relevant records to verify compliance to the information gathering policies and processes.

Our assessment will be based on engaging with management and reviewing documentation and records.

Our findings

We will discuss our findings with the business sponsor regularly throughout the review and provide you with our findings formally on conclusion of our fieldwork.

Approvals

Completion of this review is supported by:

Sponsors

Pennie Pearce
GM Information

11/04/2022

Warren Hudson
GM Integrity and Debt

11/4/2022

[1] The Information Gathering and Public Trust model standard elements that apply and are to be included in this review are the Legislative and Policy Framework element and the Implementing Strong and Comprehensive Polices and Processes section of the Organisational safeguards element

2021-22/R340

Appendix 2 – Relevant Sections of the Model Standards Subject to Review

Legislative and policy framework

Ensuring public servants' actions are lawful

Model standards:

- Agencies take the following into account in their policies, and when making decisions about information gathering:
    - - Any agency-specific legislation.
    - - The Privacy Act 1993.
    - - Any guidance issued by the Government Chief Data Steward, Privacy Commissioner or Ombudsman.
    - - Relevant decisions by the courts.
- Agencies also take into account the obligations on public servants under the State Services Commission's Code of Conduct, which mean that some ways of gathering information that are lawful for private citizens to undertake are not appropriate for public servants.
- Agencies that undertake information gathering for regulatory compliance, law enforcement and security purposes pay particular attention to the following:
    - - The protection against unreasonable search and seizure in the New Zealand Bill of Rights Act 1990.
    - - The Search and Surveillance Act 2012.

Ensuring public servants act in accordance with the State Services Code of Conduct

Model standards:

- For the avoidance of doubt it is not acceptable for an agency to:

- Classify a person or group of people as a security threat - and to use that as justification for gathering information - solely because they lawfully exercise their democratic rights (including their right to freedom of expression, association, and peaceful assembly to advocate, protest or dissent)
- Gather information about people or groups for the sole purpose of managing reputational risk to an agency.

Organisational Safeguards

Implementing strong and comprehensive policies and processes

Model standards:

• Agencies have policies and operational processes in place that describe:
- the agency's mandate to undertake information gathering activities
- the scope of activity within that mandate
- the decision-making framework and process that staff should follow when considering such activity, including when a warrant should be sought
- relevant legislation, case law, and standards (context specific)

- the support or training provided to staff
- review, accountability and oversight mechanisms
- guidance on the use, storage and destruction of any information collected.

• Agencies regularly review their legislation and policies to ensure that they provide an appropriate framework for regulatory compliance and law enforcement activities and provide advice to Ministers accordingly. The review should include completion of a Privacy Impact Assessment.

Model standards:

• Agency policies are specific about the protocols that apply to information gathering for risk assessment, compliance management or enforcement purposes (for example: what sources are appropriate and why; how information is collected and analysed, how information will be stored).
• Agency policies are clear about what steps are taken to verify information sources and validate the information source, where appropriate.
• Information provided to agencies that appears to have been obtained illegally is reported to New Zealand Police.
• Policies and training support staff working in these areas to understand and navigate the important issues of professional distance and public perception associated with the exercise of their powers.

Appendix 3 – Policy, Guidance and Process Documents

A full desk top review was made of relevant documents, policy and guidance provided by MSD. These included:

- MSD – Code of Conduct – August 2021
- Code of Conduct for Obtaining Information under Clause 2 of Schedule 6 of the Social Security Act 2018
- Code of Conduct for Obtaining Information under Section 125 of the Public and Commun ty Housing Management Act 1992
- Client Service Integrity – Stolen Identity and Privacy Breach Guidelines
- Gathering Information – Benefit and Social Housing Fraud – July 2022
- External Resources, Contractors and Consultants - Finance July 2019
- Contractors and Consultants Policy – April 2022
- Procurement Policy – March 2022
- Information Security Policy – March 2016
- Reporting a Privacy or IT Security Breach
- Acceptable Use of Technology Policy – March 2016
- Privacy and Security of Information Policy – February 2022
- Social Media Policy – December 2021
- Police Reports on Person Under Investigation and Witnesses – March 2016
- Disposing of Information Policy – August 2021
- Privacy Act 2020 Policy
- Search Warrants Policy – September 2019

- The Centralised Audit Responsibilities in FIS - 5 March 2020
- Client Services Integrity – Assurance Process April 2022
- MSD's Assurance Plan for Codes of Conduct
- Assurance Checking for Developing Staff April 2021
- Case Audit Reports template
- Stolen Identity and Privacy Breach Guidelines - December 2021
- Analyse, Interview and Decide Guidance – March 2018
- Practice Guide – Investigation Information Gathering – August 2022
- Social Media Guidance
- Disposing of Information Guidance – April 2022
- Privacy Strategy
- Privacy Act 2020 guidelines
- Official Information Act 1982 guidelines
- Requesting and Executing a Search Warrant
- Search Warrant Process Guidance
- Evidence of relationship status – 27 October 2015
- Use of Dictaphones – July 2021
- Fraud Indicators – December 2021
  Prosecution Process for Investigators – November 2021
- Use of External Security Consultants Process – June 2019

Use of publicly available information to support integrity of the welfare system

Last Review Date:	June 2024
Next Review Date:	June 2026
Approved by:	Organisational Health Committee; July 2024
Owner:	General Manager Integrity and Debt

Purpose

The Ministry of Social Development (the Ministry) recognises the value of publicly available information in supporting the investigation and prevention of fraud against the welfare system.

The purpose of this policy is to provide clear guidelines and objectives for Ministry staff seeking to collect and use publicly available information for the functions described (see **Scope**).

Publicly available information

Under Information Privacy Principle (IPP) 2 of the Privacy Act 2020 (the Act), MSD does not need to comply with the principle of collecting personal information directly from the individual concerned where it has reasonable grounds to believe that the information is publicly available.[1]

However, even when the source of the personal information is a publicly available publication, IPP 10 prevents MSD from using that information if it would be unfair or unreasonable to do so.

This policy adopts the definition of **publicly available information** used in the Act. Under section 7(1) of the Act, publicly available information is defined as "**personal information** that is contained in a publicly available publication".

A **publicly available publication** is defined as "information in printed or electronic form that is generally available to members of the public free of charge or on payment of a fee". This can include (but is not limited to) publications such as books, magazines, newspapers, public registers, and information posted publicly online.

For the purposes of this policy, publicly available online information can include information shared between individuals or groups on a **social media platform**, where access to relevant **content** is subject to only minimal access criteria (i.e. a username, password, or other simple login details) and it is clear that the content is not intended to be shared with a restricted audience.

Searches of social media platforms must only be done in accordance with the guidance set out here: Social Media Searches – Objective (A775972).

More definitions are included at the bottom of this policy (see **Definitions**).

[1] See IPP 2(2)(d) under section 22 of the Privacy Act 2020

Scope

This policy applies to the functions of the Ministry business areas responsible for the investigation and collection of overpayments, including fraudulent overpayments, and breaches of the MSD staff Code of Conduct: Integrity and Debt and Workplace Integrity (Internal Integrity).[2]

This policy is not intended to in any way bypass, override, or contradict the Ministry's existing statutory information gathering powers, or the Codes of Conduct governing their use (see **Principles**).

This policy should be read in conjunction with other related policies (see **Related policies and legislation**).

This policy is supported by specific guidance for staff (see **Related standards and guidance**).

Context

To support their functions, MSD integrity staff (see **Scope)** may, in accordance with this policy, access publicly available information about a current or former client, their family members, contacts, associates, other persons suspected of being involved in fraudulent activity against MSD, or staff who may have breached the MSD Code of Conduct.

In practice, this usually involves the collection of information from one or more of the following online or print sources:

- Search engines, such as Google
- Social media platforms, such as Facebook (Meta), X (formerly Twitter), Instagram, LinkedIn, TradeMe, and TikTok
- Public lists, registers, and databases; including the Companies Register, Insolvency and Trustee Service, electoral rolls and habitation indexes
- Information collation services procured by the Ministry; namely Infolog.

The above list is not exhaustive, and the types of sources available to staff may change as new media becomes available

Principles

The following principles are a framework for good decision-making and should be considered when collecting or using publicly available information.

Respect for privacy

MSD staff must only collect and use personal information in accordance with the information privacy principles (IPP) specified by the Privacy Act 2020 and other relevant legislation.

[2] Integrity and Debt is comprised of the following business areas: Client Service Integrity, Information and Advice, Intelligence and Integrity Insights, the Integrity Intervention Centre, and Client Support Debt Management.

When collecting and using publicly available personal information, staff should have particular regard to IPPs 1, 2, and 4:

Collection is necessary for a lawful purpose (IPP 1)

Publicly available information should only be collected where it is for a lawful purpose connected with MSD's statutory functions or activities.

In accordance with this policy, staff may collect publicly available personal information to support integrity checks, investigations, and related integrity activity, including substantiating allegations, gathering evidence to support prosecutions, and recovering overpayments.

This information may also be collected to support intelligence activity aimed at the prevention and detection of fraud and misuse, including the development of **open-source intelligence** to inform the design of integrity controls for MSD's products and services.

The investigation of internal integrity issues, such as staff fraud and breaches of the employee Code of Conduct, may also use relevant publicly available information as required.

Staff should always consider what is the least amount of personal information reasonably necessary to be collected to fulfil these purposes.[3]

Information should be collected from the person where practicable (IPP 2)

Under the Act, any personal information obtained should be collected from the individual concerned unless staff believe that the information is publicly available (or that another exception under the Act applies).

The source of the personal information collected may have an impact on the authority available under the Act for using it: if the relevant information was obtained some other way but the same information happens to now be publicly available, MSD cannot rely on the "publicly available information" authority[4] for using the information under the Act, unless another authority is found (noting that where MSD is given special statutory powers to obtain information, these powers may override some parts of the Act).

Is the collection and use fair and reasonable? (IPP 4)

The methods used to collect publicly available personal information (and the use of that information) must not only be lawful but fair and reasonable and involve the least intrusive means available.

This means that the agency that holds the information must not use it without taking reasonable steps to ensure that the information is accurate, up to date, complete, relevant, and not misleading.

---

[3] The standard for "necessary" under IPP1 is not high. See Privacy Commissioner guidance: "absolute necessity" does not need to be established, but staff should be able to explain clearly why it was reasonable to collect the personal information for the given lawful purpose.

[4] IPP10(1)(d) of the Privacy Act 2020 – this authority for using personal information is only available when the personal information has been *obtained* from a publicly available source.

Ideally, any publicly available information collected should be corroborated with other sources of information, especially if doubt exists as to its accuracy, completeness, or relevance.[5]

Steps must also be taken to ensure any personal information collected must be protected against loss and unauthorised access, use, modification, or disclosure.

As noted, personal information sourced from a public source can be used unless it would be unfair or unreasonable for the Ministry to do so. This is a quite high threshold but may apply to staff intending to use information which has been the subject of a leak (e.g. where the subject person's ex-partner has distributed intimate photographs or videos on the internet).

Where practicable, staff should minimise the collection of information about persons where the information is not relevant to the purposes for which the information is sought; and where this is unavoidable, any irrelevant information should be redacted.

Compliance with the law

Staff must ensure the collection and use of publicly available information is lawful and does not conflict with any existing legislation, internal policies, standards, regulations, or relevant Codes of Conduct.

This includes meeting legislative requirements under the Official Information Act 1982, the Privacy Act 2020, the Public Records Act 2005, and the Public Service Act 2020.

As noted, where information is not being collected directly from the person concerned, care must be taken to ensure only publicly available information is collected unless the Ministry is exercising its information gathering powers under Schedule 6 of the Social Security Act 2018 or section 125 of the Public and Community Housing Management Act 1992, subject to the Codes of Conduct governing the use of those provisions.

The relevant Codes of Conduct, and associated Ethics Framework, are publicly available here: Legislation - Ministry of Social Development (msd.govt.nz).

When collecting information from digital sources, including social media, staff should ensure that their activities are not in breach of the terms and conditions of the website, forum, service, tool, application, or electronic document from which the information was obtained.

Additionally, staff must ensure that the collection and use of publicly available information is in accordance with the MSD Code of Conduct and the Acceptable Use of Technology Policy, both of which apply to anyone who works for MSD (see **Related policies and legislation**).

Maintaining public trust

In addition to ensuring that the collection of publicly available information is lawful, staff should also consider whether their activities are consistent with the standards of conduct expected of MSD staff and of public servants in general.

[5] This is also reflected in IPP8 of the Privacy Act 2020.

Staff should refer to Te Kawa Mataaho the Public Service Commission's Standards of Integrity and Conduct; and Model Standards for Information Gathering and Public Trust (see **Related policies and legislation)**.

Related policies and legislation

- Privacy Act 2020
- Social Security Act 2018
- Public and Community Housing Management Act 1992
- Code of Conduct – Schedule 6 of the Social Security Act 2018
- Code of Conduct – Section 125 of the Public and Community Housing Management Act-1992
- Public Records Act 2005
- Public Service Act 2020
- Official Information Act 1982
- MSD Code of Conduct
- Acceptable Use of Technology Policy
- Public Service Commission's Standards on Integrity and Conduct
- Public Service Commission's Information Gathering and Public Trust Model Standards

Related standards and guidance

- Infolog Searches - Doogle (ssi.govt.nz)
- Social Media Searches – Objective (A775972).

Responsibilities

Person/Party	Responsibilities
Organisational Health Committee	Approval for the 'Use of publicly available information to support integrity activity' policy. Approval of amendments to the policy.
National Manager Client Service Integrity (CSI)	Accountable for managers in Client Service Integrity maintaining a register of approved social media accounts, profiles, and pages. Accountable for access to and use of Infolog.
General Manager Workplace Integrity/ General Manager Integrity and Debt	Accountable for managers in their respective areas maintaining a register of approved social media accounts, profiles, and pages.
Manager Internal Integrity / National Manager Client Support Debt Management / Area Manager CSI / Manager Intelligence and Integrity Insights Unit/National Manager Integrity Intervention Centre	Authorising the creation of and access to approved social media accounts, profiles, and pages for information gathering purposes in their respective areas. Maintenance of business area's register of approved social media accounts, profiles, and pages.
Ministry staff	All staff must ensure they are familiar with the policy and comply with all relevant principles and requirements when collecting or using publicly available information.

Definitions

Word/ phrase	Definition
Publicly available information	Personal information that is contained in a publicly available publication.
Publicly available publication	A publication (including a register, list, or roll of data) in printed or electronic form that is, or will be, generally available to members free of charge or on payment of a fee.
Social media platform	Internet-based tools, websites, applications, and services that enable users to interact, create and share content, or participate in social networking.

Content	Information made available by a website or other electronic medium and taking the form of video, audio, text, or multimedia.
Personal information	Information about an identifiable individual and includes information relating to a death that is maintained under the Births, Deaths, Marriages, and Relationships Registration Act 2021 or any former Act (as defined in Schedule 1 of that Act).
Open-source intelligence	Intelligence products produced from publicly available information.

Social Media Searches

1 Purpose

This guidance is specific to, and supports, and will be reviewed in line with, the Ministry Policy: *Use of publicly available information to support integrity of the welfare system* (July 2024).

It provides operational guidance on when and how publicly available information on social media platforms may be collected and used by staff responsible for the investigation and collection of overpayments (including fraudulent payments) and internal integrity issues i.e. the business areas that are currently referred to as Integrity and Debt[1] and Workplace Integrity (Internal Integrity).

2 Publicly available information

To support their functions, staff to whom this guidance applies may access publicly available information on social media, including information, about current or former clients, their family members, associates, or other persons suspected of being involved in fraudulent activities against the Ministry.

It can also be used to support an investigation of internal integrity issues (e.g employee fraud and breaches of the Code of Conduct) and may also be collected as part of intelligence gathering activity aimed at understanding methods used to exploit MSD's products and services.

Definitions of key terms, such as 'publicly available information', social media platform', 'personal information', and 'content', can be found in the Ministry Policy *Use of publicly available information to support integrity of the welfare system* (July 2024).

3 When information may be considered publicly available and collected from social media?

Whether personal information on a social media platform is publicly available information is something that needs to be carefully considered in the circumstance of the particular case. Where it is clear that an individual intended to share personal information with only a restricted audience (rather than the general public), then there is a risk that the information is not publicly available information (notwithstanding that staff are able to access the information).

Where the information is not publicly available information or the use of publicly available information would be unfair on reasonable, staff cannot collect the information without identifying another legal authority for doing so (such as scheduled 6 of the Social Security Act 2018).

Indicators that content on social media can be treated as publicly available information include where:

- The social media page is fully public (e.g. no account on the platform is needed to view the information)
- The social media page is accessible to all users on the platform (where users can join the platform simply by providing basic log-in details, such as a username and email address)
- The content is published within an open group on a social media platform (an open group is a group to which any user is able to join without approval from another user).

[1] Integrity and Debt is comprised of the following business areas: Client Service Integrity, Information and Advice, Intelligence and Integrity Insights, Integrity Intervention Centre, and Client Support Debt Management.

Indicators that content on social media should not be treated as publicly available information:

6(c)

If you are unsure whether content on social media constitutes publicly available information or you have doubts about whether it is fair and reasonable to use that information, you should seek advice from your manager, the MSD Information Group, and/or MSD Legal.

4 Creation and use of social media accounts, profiles, and pages

An account should not be created, accessed, or used by staff to whom this guidance applies unless they have good reason to believe that the platform contains information relevant to the functions in scope of the Ministry Policy: *Use of publicly available information to support integrity of the welfare system* (July 2024).

Staff must obtain authorisation before creating or otherwise using (for the first time) a social media account, profile, or page to collect publicly available information for integrity purposes.

The creation of a new account, profile or page must be authorised by (as relevant to the staff member) the Manager Internal Integrity, the National Manager Client Support Debt Management, Manager Integrity and Integrity Insights, or Area Manager Client Service Integrity.

First-time use of an existing MSD account, profile, or page should be authorised by the relevant manager as outlined in the policy: *Use of publicly available information to support integrity of the welfare system*.

When using accounts, profiles, or pages to undertake searches of publicly available information, staff must adhere to the terms and conditions of the platform being used.

6(c)

Account, profile, and page characteristics

Staff should ensure that any account, profile, or page created:

- adopts a username, account name, or page name that identifies it as being owned and operated by MSD (e g. MSD Client Service Integrity 1)

6(c)

6(c)

[3] Facebook's complete Terms of Service can be found here: Facebook

[4] Facebook treats profiles, Pages, and groups as separate entities, although users must have a profile to create a page or group, or to help manage one: Differences between profiles, Pages and groups on Facebook | Facebook Help Centre

- 6(c)
-

Please note, MSD staff are not permitted to use any personal or unauthorised social media accounts, profiles, or pages for official MSD purposes. Nor are they permitted to use an authorised MSD account, profile, or page for personal purposes.

6(c)

Sending a private message

As noted, an account, profile, or page created for integrity purposes should generally not be used to communicate or in any other way interact with the other users of a social media platform.

However, in limited circumstances, staff are permitted to send a direct, private message to another user in order to request that they get in contact with MSD, but only when:

- there is a reasonable belief that that user holds information relevant to an MSD investigation or is a potential witness
- repeated attempts to contact that user by phone, letter, or email have been unsuccessful (or their contact details are not held by MSD); and
- the social media platform has a function that enables users to send and receive private messages (i.e. messages that cannot be seen by other users)

When using social media messaging applications, staff should be transparent about their identity, role, and purpose in communicating with prospective witnesses or other members of the public.

Maintaining a profile register

To keep a record of social media accounts, profiles, and pages in use, business areas and/or Client Service Integrity (CSI) regional areas must each maintain a *Profile Register* of approved social media profiles.

For each social media account, profile, or page created, the following information must be recorded in the register:

- social media platform
- username (and/or first and last name)
- password and date of last password change
- profile photo (if required)
- staff member(s) approved to use the account, profile, or page
- name of MSD page owners and administrators (if applicable)
- name of authorising manager
- date of approval
- date of account, profile, or page creation

Maintenance of each area's register is the responsibility of the authorising manager. The National Manager Client Service Integrity is accountable for authorising managers maintaining their area's Profile Register in CSI, and the General Manager Integrity and Debt and General Manager Workplace Integrity are accountable for authorising managers maintaining registers in Integrity and Debt and Workplace Integrity, respectively.

Maintenance of a Profile Register should include:

- ensuring approved accounts, pages, and profiles are captured at the time of approval and creation
- ensuring all details required to create an account, profile, or page are appropriate for use
- ensuring staff members approved to use any account, profile, or page have read and understood the Policy governing their use
- periodically reviewing the register to ensure approvals and accounts, profiles, and pages are still required and relevant
- ensuring appropriate off-boarding and that passwords to accounts, profiles, and pages are changed when a staff member with access to them changes roles or leaves MSD.

Collection and storage

For general information regarding the proper collection and storage of publicly available information, please refer to the Ministry Policy: *Use of publicly available information to support the integrity of the welfare system.*

To ensure digital information is protected and that staff maintain a record of their activities, any information collected must be captured using an approved MSD software (e.g. Snagit) and stored in an appropriate MSD repository, such as the Investigation Management System (IMS) when it includes personal or other information relevant to an integrity response, or Objective (or other MSD approved information management system).

Staff should ensure any private messages sent via a social media platform (see ***Sending a private message***) are captured using a screenshot and saved in the appropriate MSD repository (i.e. IMS or Objective).

When conducting open-source intelligence gathering, staff must redact, obscure, or anonymise any information that might identify an individual.

In general, personal information should only be stored outside of core client management systems (including IMS) when there is a legitimate business reason to do so.

Please note that failure to protect personal information held by the Ministry against unauthorised or accidental access, disclosure, alteration, loss or destruction may constitute a privacy breach.

MINISTRY OF SOCIAL DEVELOPMENT
TE MANATŪ WHAKAHIATO ORA

Memo

To: Organisational Health Committee

From: Josie Smiler, General Manager Integrity and Debt

Date: 11 July 2024

Security level: **In Confidence**

This contains legal advice and is legally privileged. It should not be disclosed on an information request without further legal advice

---

Use of publicly available information to support integrity of the welfare system

Action: **For approval**

Purpose

1 To seek approval for a policy on the use of publicly available information to support integrity of the welfare system.

Commitment to Māori

2 In the past Māori have been disproportionately impacted by our integrity and enforcement processes;

2.1 Mana Manaaki – A positive experience every time – we support MSD to prevent, detect and respond early to integrity risks, to reduce the harm caused to individuals, whānau and communities

2.2 Kotahitanga – Partnering for greater impact – we engage on our practices, approach and the outcomes we want to achieve to support MSD's strategic shifts

2.3 Kia Takatū Tātou – Supporting long-term social and economic development – our shift towards fraud prevention aims to reduce the harm caused by non-compliance.

Recommendations

3 It is recommended that you:

3.1 **Note** that Integrity and Debt have prepared a policy to govern MSD's collection and use of publicly available information for integrity purposes, with supporting guidance for staff undertaking searches of social media platforms

3.2 **Note** that the policy is not intended to in any way bypass, override or contradict existing statutory information gathering powers, or the Codes of Conduct governing their use, and refers (where relevant) to related legislation, policies, guidelines, and external regulations

3.3 **Note** that there are risks associated with MSD's searches of social media platforms, but the proposed use in the policy does not include the use of 'discreet' profiles 9(2)(h)

3.4 **Agree** to approve the attached policy: *Use of publicly available information to support integrity of the welfare system*

Context

4 Integrity and Debt[1] and Workplace Integrity – the MSD business areas responsible for the investigation of benefit overpayments (including fraudulent overpayments) and internal integrity issues (including breaches of the MSD employee Code of Conduct) – regularly use publicly available information[2] to support their functions.

5 In practice, this could involve the collection and use of information from one or more of the following online or print sources:

- Search engines, such as Google
- Social media platforms, such as Facebook (Meta), X (formerly Twitter), Instagram, LinkedIn, Trademe, and TikTok
- Public lists, registers, and databases; including the Companies Register, Insolvency and Trustee Service, electoral rolls, and habitation indexes
- Information collation services procured by the Ministry, namely Infolog.

[1] Integrity and Debt is comprised of the following business areas: Client Service Integrity, Information and Advice, Intelligence and Integrity Insights, the Integrity Intervention Centre, and Client Support Debt Management.

[2] Under section 7(1) the Privacy Act 2020, publicly available information is defined as 'personal information that is contained in a publicly available publication', with a publicly available publication being defined as 'information in printed or electronic form that is generally available to members of the public free of charge or on payment of a fee.'

6 This information can play a significant role in integrity checks, interventions, investigations, and related integrity activity, including gathering evidence to support prosecutions and the recovery of overpayments.

7 It is also used by MSD to support the investigation of internal integrity issues (e.g. employee Code of Conduct breaches) and may also be collected as part of intelligence gathering activity aimed at understanding methods used to exploit the Ministry's products and services.

8 According to the Privacy Act 2020, the Ministry need not comply with the general principle of collecting personal information directly from the person concerned where it has reasonable grounds to believe that the information is publicly available.[3]

9 However, as an agency, MSD's collection and use of that information is subject to and, in some cases, restricted by a range of legislation, internal policies, and public sector regulations. These include the Privacy Act 2020, MSD's Code of Conduct, and the Public Service Commissioner's Information Gathering and Public Trust Model Standards.

10 In March 2017, the Ministry approved the *Interim Social Media Guidelines*, which permitted intelligence analysts to adopt a pseudonym when searching publicly available content on social media platforms, so as to minimise the risk of being identified. However, the Ministry suspended this practice in 2021, following an independent review of the MSD's information gathering processes and controls.[4]

11 Since that time, all MSD staff undertaking integrity work have adhered to the following collection principles when searching social media platforms:[5]

11.1 The information must be available to the general public – no form of deception or entrapment should be used to gain access to the information (e.g. adding a client as a 'friend' on Facebook or using a fictitious username for MSD accounts)

11.2 Staff must have 'reasonable cause' to suspect that a person may have committed an offence or obtained by fraud any payment, credit, or advance, in order to gather social media information

11.3 Staff should not rely on social media information; it should be corroborated with other evidence.

---

[3] See Information Privacy Principle 2: Privacy Act 2020 No 31 (as at 06 December 2023), Public Act Contents – New Zealand Legislation

[4] *Assessment of Information Gathering Process and Controls* (Ernst and Young, September 2021).

[5] See Investigative techniques - Doogle (ssi.govt.nz).

12 However, we believe our staff might benefit from more comprehensive guidance on the collection and use of information from public sources, both digital and non-digital, but especially in relation to searches of social media, which is a dynamic and rapidly evolving landscape.

13 This was reinforced by research through the Ian Axford Fellowships in Public Policy, *Social media monitoring by New Zealand agencies: policy and legal landscape, risks, and considerations*, published in June 2024.[6] The research noted previous practices by MSD, prior to the independent review in 2021, and found that MSD does not currently have a policy in place governing searches of social media platforms.

14 The Office of the Privacy Commissioner has also expressed that agencies must be cautious in their collection of publicly available information from a social media platform[7].

We have prepared a policy on the use of publicly available information for integrity purposes

15 We have prepared a policy on the collection and use of publicly available information for integrity purposes, applicable to the functions of Integrity and Debt and Workplace Integrity.

16 Appendix 1 provides the policy, *Use of publicly available information to support integrity of the welfare system*, for your approval.

17 It aims to provide clear guidance and objectives for specific MSD staff undertaking searches of public sources, with reference to three good-practice principles: respect for privacy, compliance with the law, and maintaining public trust.

18 The policy is not intended to in any way bypass, override or contradict existing statutory information gathering powers, or the Codes of Conduct governing their use.

19 The policy refers (where relevant) to related legislation, policies, guidelines, and external regulations, including the MSD Code of Conduct, and the Public Service Commission Te Kawa Mataaho Standards on Integrity and Conduct and Information Gathering and Public Trust Model Standards.

20 Accompanying the policy, comprehensive guidance has been developed for the collection and use of publicly available information from social media

[6] Social media monitoring by New Zealand agencies: policy and legal landscape, risks, and considerations – axfordfellowships.org.nz

[7] See AskUs | Article | What is publicly available information? | Office of the Privacy Commissioner and If I'm not doing anything wrong, what do I have to hide? (youtube.com).

platforms specifically, including on the creation and use of social media accounts, profiles, and pages by relevant MSD staff. This does not allow for the use of 'discreet' profiles i.e. a profile or account that cannot be identified as being owned and operated by the Ministry by, for example, using a pseudonym or other fictitious account information to collect publicly available information.

21 Appendix Two provides this guidance, *Social Media Searches*, to support the policy if approved.

We have considered the risks associated with MSD's searches of social media platforms

22 While several agencies permit their staff to login to accounts and profiles in order to collect information from social media platforms for law enforcement purposes, other agencies limit use to information that can be accessed without logging on to the platform.

23 As noted, social media platforms can be an important source of publicly available information for our integrity staff, and Facebook (Meta) is currently the platform most frequently used in MSD's interventions, integrity checks, and investigations.

24 To ensure compliance with Facebook's Terms of Service (the Terms), our social media guidance requires staff to use an authorised MSD Facebook 'Page' rather than a profile when undertaking searches of the platform.[8] Facebook is clear that their accounts and profiles can only be used for personal purposes and that the use of the platform by a government organisation should be through a Page instead.

25 Staff are also cautioned against accessing closed or private groups – i.e. where access and membership is controlled by another user – as the fact the group is closed suggests that members only intended to share the information with a restricted audience (and not the general public). Accordingly, MSD would have no legal authority to access such information and doing so would create a high risk of breaching the Privacy Act 2020.

26 Some operational considerations will need to be given for relevant staff to utilise any such Facebook Pages – this is because a personal profile is required to log in to the Page to undertake the integrity activity. This may mean we limit social media searches via these pages to select staff who

[8] Facebook treats profiles, Pages, and groups as separate entities, although users must have a profile to create a page or group, or to help manage one: Differences between profiles, Pages and groups on Facebook | Facebook Help Centre

6(c)

9(2)(h)

27

28

29

Next steps

30 If approved, the policy and associated social media guidance will be finalised, and both documents will be uploaded to the relevant business groups' knowledge bases (Doogle).

31 We expect a policy implementation and transition period of up to three months, during which time:

- Integrity and Debt and Workplace Integrity staff will be notified of the changes and staff training needs in respect of the policy will be assessed with Learning and Capability Development
- Social media profiles and logins currently in use by integrity staff will be audited to ensure compliance with the policy; and

9(2)(h)

- Profile registers will be prepared in consultation with the relevant Integrity and Debt and Workplace Integrity managers, in line with the roles and responsibilities defined in the guidance.

Consultation

32 The policy and associated guidance were developed in consultation with MSD Legal, the Information Group, Communications and Engagement, Workplace Integrity, and Integrity and Debt managers (Client Service Integrity, Intelligence and Integrity Insights, Client Support Debt Management, and the Integrity Intervention Centre). 9(2)(h)

Appendices

Appendix One Policy - *Use of publicly available information to support integrity of the welfare system*

Appendix Two Guidance - *Social media searches*

Author: Out of scope Senior Advisor, Integrity and Debt
Responsible manager: Out of scope Team Manager Information and Advice, Integrity and Debt.

Advisory review – Assessment of Information Gathering Processes and Controls: Action Plan

The following action plan provides an overview of managements comments and proposed actions in relation to the findings and recommendations made by EY in their report "Assessment of Information Gathering Processes and Controls". Fieldwork undertaken by EY in May – July 2021, report finalised in September 2021.

Finding	Recommendation	Management comment / proposed actions	Expected completion date	Responsibility	Oversight / monitoring by	Status	Follow-up comments	Last updated
The development of a Target Operating Model ("TOM") in 2020 included a deep dive into the Intelligence Unit. The recommendations within the TOM include mechanisms to improve the governance and oversight of information gathering activities. The implementation of this TOM would lift already established mechanisms and create new ones to effectively mitigate the risks inherent in information gathering activities.	**Complete the implementation of the future state operating model as it relates to the Intelligence Unit, and resource accordingly** - We are supportive of the direction the future state operating model for Integrity and Debt Services is taking in relation to the Intelligence Unit, in particular, recommendations to; create additional capacity for an Insights & Analytics capability, provide technical oversight, professional development, and coaching to the intelligence team, to implement and leverage advanced analytic techniques, and to transition from a responsive model to a prevention focused model. In the drive toward preventative intelligence gathering activities, standing up the future operating model is a critical step.	Implementation of a broader strategy for Integrity and Debt is already underway. This strategy links to MSD's wider strategy (TPT) and will support implementation of the changes outlined in the target operating model. The target operating model is expected to be implemented over the next 2 to 5 years.	N/A	Warren Hudson, GM Integrity and Debt	Regular reporting to the Service Delivery LT, Leadership Team and OHC on the implementation of the broader strategy for Integrity and Debt already exists. Further reporting is therefore, not considered necessary.	**Closed** – work is in train to support implementation of the broader strategy for Integrity and Debt and this is being monitored separately and existing arrangements are in place to monitor implementation. No further work for this action is considered necessary.	N/A	
The Intelligence Unit have a 'Handbook' which acts as a central repository for all key process documentation. This handbook is maintained by the Senior Intelligence Analyst and is used to guide and direct work. It is also used to onboard and train new team members from time to time. Notwithstanding this, many of the processes and practices documented in the Handbook are outdated and are at varying degrees of quality. The lack of up-to-date and comprehensively documented processes opens the Ministry to the risk that information gathering practices don't align to	**Review and update information gathering processes and practices** - The Intelligence Unit should conduct a full review of processes and practices that guide and direct its information gathering activities. Documented processes and practices should align with and support the implementation of the future operating model.	Implementation of this is underway.	31/10/2021	Out of scope Manager Intelligence Unit	Information Group dashboard reporting to OHC	**Underway**		

Finding	Recommendation	Management comment / proposed actions	Expected completion date	Responsibility	Oversight / monitoring by	Status	Follow-up comments	Last updated
current practice or the Ministry's legal and ethical obligations.								
The 'Interim Social Media Use Guidelines' were created in March 2017 and have not been reviewed or updated since. This document details the process of searching for publicly available information on social media platforms through the use of a skeleton profile. Current practice dictates this profile has no picture, no pages linked, and requires a fake name and email address to be set up. While the information gathered by these means is open source, the use of pseudo profiles can be viewed as deceptive and underhanded. It can also be seen as a breach of the terms and conditions of various social media platforms.	**Complete the investigation into pseudo social media profiles and obtain a legal opinion on using social media as a source of information -** Guidelines over creation and use of social media accounts must align to the Ministry's current policy, and regulations applicable to the public sector. Legal counsel over the use of social media will ensure privacy risks are effectively mitigated to an acceptable level. A full review of the practices for gathering information from social media must also be considered.	This practice was ceased in June 2021. Since this time the Intelligence Unit have applied the same approach as Fraud Intervention Services. Legal advice is being sought, which will be used to inform future practice. The Intelligence Unit have reached out and an inter-agency working group is being formed to work on Social Media guidelines across government.	TBD – working group is now established and interagency work is set to commence 06/10/2021	Out of scope Manager Intelligence Unit	Information Group dashboard reporting to OHC	**Underway**		
While the Intelligence Unit have established document management and archiving practices for its cases, there is no guidance (for example, frequency of review) pertaining to the maintenance of the Intelligence Unit's processes. This creates a risk that the information gathering practices of the Ministry are not aligned with current practice, governing legislation and regulations, or recommendations of the OPC Inquiry.	**Establish robust document control mechanisms, including processes to independently review information gathering practices that could compromise public trust -** The Intelligence Unit should consider implementing a regular review and update of documented processes and practices. Current practice and regulation are always evolving. Documented practices should evolve in line with changes to the legal environment. Processes and practices must also align with the risk appetite of the Ministry and therefore changes to high risk information gathering practices should be independently reviewed.	Implementation of this is underway.	15/10/2021	Out of scope Manager Intelligence Unit	Information Group dashboard reporting to OHC	**Underway**		
The development of a Target Operating Model ("TOM") in 2020 included a deep dive into the Intelligence Unit. The recommendations within the TOM include mechanisms to improve the governance and oversight of information gathering activities. The implementation of this TOM	**Ensure there is shared understanding of how risks inherent to the Ministry's information gathering activities are managed to acceptable levels** - A shift toward the new operating model will bring new risks for the Ministry, especially in terms of client privacy with the	Implementation of a broader strategy for Integrity and Debt is already underway. This strategy links to MSD's wider strategy (TPT) and will support implementation of the changes outlined in the target operating model.	N/A	Warren Hudson, GM Integrity and Debt	Regular reporting to the Service Delivery LT, Leadership Team and OHC on the implementation of the broader strategy for	**Closed** – work is in train to support implementation of the broader strategy for Integrity and Debt and this is being monitored separately and existing arrangements are in	N/A	

Finding	Recommendation	Management comment / proposed actions	Expected completion date	Responsibility	Oversight / monitoring by	Status	Follow-up comments	Last updated
would lift already established mechanisms and create new ones to effectively mitigate the risks inherent in information gathering activities. The Fraud Referrals and Investigation Allocation Business Process outlines a clear escalation process within the Intelligence Unit. Risk escalation factors include cases where there could be reputational risk to the Ministry, involvement of gangs or organised crime groups, public safety concerns, staff safety concerns, among other things. Consideration is also given to the definition of high-risk cases which may include those that involve identity fraud, a previously unseen modus operandi, a system, policy, or procedural loophole, among other things. Where risk escalation factors or high-risk cases are identified, cases are able to be escalated within the Ministry based on the significance of the risk. The business process document also stipulates the roles and responsibilities at each level within the information gathering processes. This document has not been updated since 2015.	introduction of more prevention focused activities. Changes to the activities within the Intelligence Unit need to include conversations with wider units of the Ministry to ensure the risks involved are appropriately mitigated. This includes the design and implementation of processes and practices that govern these activities.				Integrity and Debt already exists. Further reporting is therefore, not considered necessary.	place to monitor implementation. No further work for this action is considered necessary.		
The Intelligence Unit have a strong Quality Assurance ("QA") process that includes two levels of review. An initial QA is completed by the Principal Intelligence Analyst ("PA") which is followed by secondary QA by the Senior Intelligence Analyst ("SA"). Each have a slightly varied focus to ensure that all parts of the QA process are followed. The success of the QA process is also underpinned by the culture within the unit. The PA and SA make a point to know the Intelligence Analysts ("IA") well and understand their	**Adopt a risk-based approach to reviewing and approving intelligence products -** The Intelligence Unit should prioritise QA of products based on the level of risk associated. Having two in-depth QA reviews is not necessary for all the intelligence cases. Detailed QA by multiple levels should be reserved for activities where there is a higher level of judgment needed or complexity involved.	We do not agree with this recommendation. The approach, as described in the finding, is inaccurate. Quality assurance reviews are performed by the PIA. The SIA review is a high-level check prior to sending out information – it is not a detailed quality assurance check. We believe our current approach is appropriate and will therefore continue with our current practice.	N/A	Out of scope Manager Intelligence Unit	Information Group dashboard reporting to OHC	**Closed** – accept that the recommendation will not be implemented. The approach to and level of quality assurance occurring within the Intelligence Unit is considered appropriate.		

Finding	Recommendation	Management comment / proposed actions	Expected completion date	Responsibility	Oversight / monitoring by	Status	Follow-up comments	Last updated
individual strengths and weaknesses.								
The Intelligence Unit have created written scripts to extract data from Ministry source systems. The Data Scientists within the unit have built statistical models for early detection and data mining. Their ability to gather information internally is enhanced by the Data Scientists and other employees who have in-depth knowledge and skills required to perform data sweeps over the central Ministry database. The IMS tool is used to support information gathering activities by keeping records of intelligence cases and the information gathered throughout this process. However, the view exists that the tool lacks the appropriate functionality to effectively support the end to end activities of the Intelligence Unit or support enhanced information gathering activities. CaseTool is a platform created by the Intelligence Unit that acts as a work-around to provide additional functionality that does not exist in IMS to help support activities. However, there is a disconnectedness that arises from the lack of an appropriate tool to support end to end information gathering activities.	**Investigate where improvements can be made to exiting systems and tools -** The tools available to the Intelligence Unit, namely IMS, Objective, and CaseTool, are disaggregated and, in their view, fail to adequately support the wider activities that are performed. If this view is shared with Fraud Integrity Services and Internal Integrity, consideration should be given to identifying opportunities to implement tools that support the end to end case management, especially the more complex activities that will follow the implementation of the new operating model design. Any changes will need to be considered in conjunction with the Ministry's wider change portfolio.	Implementation of a broader strategy for Integrity and Debt is already underway. This strategy links to MSD's wider strategy (TPT) and will support implementation of the changes outlined in the target operating model. The tools used by the Intelligence Unit and the wider Integrity and Debt Group may be considered as part of this strategy, however, any changes will be dependent on the availability of resources given the number of priority change portfolios and programmes underway.	N/A	Warren Hudson, GM Integrity and Debt	Regular reporting to the Service Delivery LT, Leadership Team and OHC on the implementation of the broader strategy for Integrity and Debt already exists. Further reporting is therefore, not considered necessary.	**Closed** – work is in train to support implementation of the broader strategy for Integrity and Debt and this is being monitored separately and existing arrangements are in place to monitor implementation. No further work for this action is considered necessary.		
Objective (formerly, EDRMS) is a central document repository that is available to the Intelligence Unit to store information gathered through intelligence activities. However, most intelligence analyst archive cases, and associated attachments, on the E:drive rather than Objective. Locations where cases are stored have access restricted exclusively to employees within the Intelligence Unit. Interviews	**Shift to using Objective for archiving cases and relevant artefacts -** Objective provides a platform for effective archiving of personal sensitive information gathered by the Intelligence Unit. However, many within the Intelligence Unit continue to use the E:drive to store cases and related sensitive personal information that has been gathered. It is recommended that the Intelligence Unit shift to using Objective for holding and	This recommendation went live on 27/09/21 and will be monitored. Objective training will be delivered to staff within the Intelligence Unit to ensure this change is implemented successfully.	N/A	Out of scope Manager Intelligence Unit	Information Group dashboard reporting to OHC	**Completed** – transition to Objective has already occurred.		

Finding	Recommendation	Management comment / proposed actions	Expected completion date	Responsibility	Oversight / monitoring by	Status	Follow-up comments	Last updated
revealed a desire to shift the archiving of cases from E:drive to Objective. Using objective to archive intelligence cases would ensure the Intelligence Unit's information management processes align with those of the wider Ministry.	archiving intelligence cases. Using objective to archive intelligence cases would ensure the Intelligence Unit's information management processes align with those of the wider Ministry.							

Investigative techniques

This page provides information and resources for Client Service Integrity staff relating to investigative techniques.

On this Page:

Out of scope

Social media

Gathering information from social media is an acceptable investigation technique and may produce evidence to support criminal offending.

Collection Principles:

The information must be available to the general public No form of deception or entrapment should be used to gain access to information. E.g. adding a client as a ‘friend’ on Facebook.

You must have ‘reasonable cause’ to suspect that a person may have committed an offence or obtained by fraud any payment, credit or advance in order to gather social media information.

You should not solely rely on social media information; it should be corroborated with other evidence.

In order to view many social networking sites such as Facebook an account is required. Fake aliases should not be used as it breaches the terms and conditions of social networking sites and may give the perception the information was improperly obtained.

6(c)

You may ask witnesses to voluntarily provide social media information that they already have access to, which would form part of their witness statement. You should not deliberately circumvent the policy by asking a third party to use deception or entrapment to access information that the third party does not already have already have legitimate access to e.g. requesting someone to add a client as a ‘friend’ on Facebook.

Out of scope

Out of scope