23 February 2022

Members
Security & Intelligence Board

Revision of the Classification System Policy 2022

Executive summary

1. The purpose of this paper is to seek SIB agreement and approval for proposed changes to the Classification System policy to address the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain (RCOI) recommendations on Information Sharing (Recommendation 9).
2. We bring this change for approval to SIB as the steward of the Protective Security Requirements (PSR) including the Classification System. As steward, SIB provides leadership and vision of the PSR and promotes good protective security policy and practices across government.
3. The structure, levels and definitions of the New Zealand Government Information Security Classification System (Classification System) are not changing as a result of this project as simplification of the system was not included in the RCOI recommendations.
4. Instead, this project rethinks the policy which forms the foundation of the Classification System to drive wider systems and culture change across government in support of achieving the RCOI recommendations. It clarifies and strengthens current protective security requirements on what agencies should already be doing.
5. The areas that have been strengthened in the proposed policy include:
    a. Introduced higher level policy principles and expected behaviours by agencies and their people aligned to the current legislation that governs government information.
    b. Added principles and policies to support the RCOI recommendations including information sharing and declassification.
    c. Reframed, strengthened and clarified the policy and existing requirements under each of the principles to enable agencies to drive the behavioural change within their organisations.
6. The project is still in progress and due for completion by end June 2022. If the policy is approved, the project will complete and deliver clear guidance, education and training materials, and tools and templates to support agencies to implement the policy within their organisations.

7. By itself, this project will not realise the full objectives sought by the RCOI. The policy sets out expectations for good practice but agencies will need to assess how they achieve the policy intent, implement the recommended practices and supplied training materials, and encourage the behavioural changes within their organisations.
8. The revised policy will come into force July 2022 and fully replace the existing policy over a transition period of 2 to 3 years. Also by July 2022, all guidance, education materials, tools and templates will be delivered and central support for agencies to implement the changes will be delivered through the NZSIS PSR function.
9. Agencies may need to set up a project to implement the revised policy. The size and costs of the project will depend on the nature of the impacts on their existing practices. For some agencies who already follow the existing Classification System policy and have good classification, declassification, and information sharing policies, procedures, and education in place, the impacts should be relatively minor. For others where capability needs to be built, the impacts may be more substantial and may require additional resources and funding to implement. The planning for this should be integrated into the agency's annual protective security improvement programme.

Background

10. Cabinet agreed to the current Classification System in December 2000. [CAB(00)M42/4G(4)]
11. The purpose of the Classification System is to define how government information is classified to ensure it is appropriately used, managed, and protected.
12. In 2018, SIB commissioned a review of the Classification System led by NZSIS on the back of the September 2018 report by the Inspector-General of Intelligence and Security (IGIS) on the Classification System. The IGIS found that the Classification System is inconsistently applied, and is not well understood or supported by effective systems or processes across wider government. The IGIS made recommendations to:
    a. simplify the classification system to make it easier to get classification right
    b. introduce a regime and practices for systematic declassification
    c. develop a training programme to accompany the classification system reform
    d. build and use a set of indicators for assessing classification system function and performance.
13. The purpose of the NZSIS-led review was to understand the appetite for change across government, to design a more fit-for-purpose and simplified Classification System, and to assess impacts on government of changing the Classification System. This review found a strong appetite for change of the Classification System and support for the IGIS' findings, designed a simplified 4-level Classification System, and analysed two options:

a. Option A – Improved, standardised, and centralised education on the current Classification System; and Option B – Change to the simplified 'fit for purpose' Classification System, with standardised education.

b. Option B was the overwhelmingly preferred option by 20 of 21 reference agencies and was supported by members of the Security and Intelligence Board in October 2020. It had an indicative 20 year cost of $35 million (spread across 39 agencies), and a net present value of $55 million and return on investment within 6 years.

14. The RCOI report was published on 8 December 2020 making recommendations for change to the Classification System within Recommendation 9 (Information Sharing). Recommendation 9 said:

> *"We recommend that the Government:*
>
> ***Direct** the new national intelligence and security agency (Recommendation 2), and in the interim the Department of the Prime Minister and Cabinet, to improve intelligence and security information sharing practices, including:*
>
> *9 (a) driving a change in approach to the "need-to-know" principle across relevant Public sector agencies, with special attention given to local government including the emergency management structures at the local and regional level, to ensure it enables rather than just restricts information sharing; and*
>
> *9 (b) overseeing the implementation, within six months, of recommendations in the 2018 Review of the New Zealand Security Classification System:*
>
> *i. expanding the classification system principles to provide that no information may remain classified indefinitely and that, where there is doubt as to the classification level, information is classified at the lower level;*
>
> *ii. revising and strengthening Public sector agency guidance and developing training;*
>
> *iii. adopting a topic-based approach to systematic declassification of historic records; and*
>
> *iv. developing indicators of function and performance of the classification system."*

15. The RCOI was unaware of the findings of the NZSIS-led review. The RCOI report recommended implementation of most of the IGIS recommendations but omitted the requirement to simplify the Classification System. Their recommendations were effectively to undertake Option A with emphasis on revising the policy principles to enable better information sharing and information declassification.

16. The Government has agreed in principle to implement all of the Royal Commission's recommendations, noting that implementing some of the recommendations will require further consideration.

17. A budget bid for 21/22 was approved to undertake a project to design and implement the RCOI Information Sharing recommendation. [CAB-21-MIN-0116.34].

18. Although simplifying the Classification System was not approved for inclusion in 21/22 financial year, the findings of the NZSIS-led review is that it is still critical to be completed in the future to achieve the desired objectives and vision for the

Classification System. A separate budget bid is being considered to continue the simplification work in the 22/23 financial year.

Project vision, scope and assumptions

19. The RCOI Information Sharing project was initiated in July 2021 and will be completed by June 2022. Through the initial phase, the project team worked with reference agencies to better understand the problems identified by the RCOI and IGIS, identify the behaviours that need to change and identify what needs to be developed or clarified to bring about the change. A vision was agreed and project scope and deliverables identified to establish the right conditions to enable the vision to be achieved.

Vision: A Classification System that protects and benefits all New Zealanders

20. The Classification System vision – to enable stewardship of government information for the benefit of all New Zealanders - He taonga te parongo, tukuna kia tina.
21. Our vision is to have a Classification System:
    a. that enables and supports the appropriate classification and systematic declassification of government information to improve government transparency and accountability to the public
    b. that propels information-sharing and purposeful collaboration between those who need it, when they need it
    c. where all government information is appropriately protected and used to its full potential
    d. where stewardship of government information benefits all New Zealanders.

Project scope and implementation assumptions

22. This project rethinks the foundation of the Classification System to drive wider systems and culture change across government. It clarifies and strengthens current protective security requirements on what agencies should already be doing.
23. The project will not change or simplify the classification levels or definitions or change the underpinning secure handling markings or requirements. It also does not implement the policy within agencies but provides the guidance and standard tools that can be used by agencies to implement it within their own environment. The project also will not change any existing legislation but will leverage and reference existing requirements, practices and tools.
24. The project scope includes the delivery of the revised policies and guidance, supporting tools, processes, and standardised training packages required to enable agencies to adopt and implement the revised Classification System policy. The aim of the deliverables will be to deliver standard tools, exemplars, and content that will drive

greater consistency across government while enabling agencies to tailor the programme to their specific environment, information, and policy choices.

25. Systems and culture change take time. The project will develop implementation, change and communication management, and train-the-trainer packages will be delivered in May and June 2022 to enable the PSR team and other participating community of practice agencies to support the implementation across government over the next few years.

26. It will be the responsibility of agencies to embed the revised policy or strengthen their existing policies within their organisations as part of their current protective security improvement programme. Agencies will be able to begin implementation from July 2022 onwards. We expect that it will take 2 to 3 years to implement across mandated agencies.

27. Mandated organisations will need to report back on their plan and status of their classification system programmes in March 2023 and begin measuring the classification system performance in the March 2024 PSR self-assurance report. The project will also provide classification performance measurement guidance alongside revisions to the PSR capability maturity model, self-assessment and reporting process, and moderation framework.

Policy revision, consultation, and feedback

28. Classification System good practice already exists in pockets across government. From August 2021, the project team continues to engage with identified reference agencies and international partners who already undertake good practice surrounding the classification system, education, performance measurement, declassification, and information sharing to learn from, re-use, adapt and test existing practices.

29. The Classification System must support and align with the wider New Zealand government information management system. In August and September 2021, the project team engaged with the Chief Ombudsman, Chief Archivist, and Privacy Commissioner and their teams to ensure any changes proposed to the Classification System enabled and supported core legislation and existing standards.

30. The Classification System must support and enable better information-sharing across the national security and national emergency management systems. The project team is also engaging with DPMC, National Emergency Management Agency, and other local government to ensure that the policy and guidance aligns and enables the information-sharing practices as envisioned by the RCOI.

31. In October 2021, an initial draft of the revised policy was developed and reviewed within the NZIC, RCOI Steering Group members, and PSR Governance Group members.

32. On 16 November 2021, a discussion document with the final draft of the policy was submitted widely across both mandated and non-mandated agencies seeking feedback on the proposal. Consultation initially closed on 22 December 2021; however,

we did another final push for any last minute feedback and formally closed the consultation on 12 January 2022.

33. 32 agencies responded to the request for feedback (Appendix E.) A majority of agencies were in support of the policy; however, common concerns and questions were raised and summarised in Appendix D: Agency Feedback Themes. The final policy in Appendix A has been revised based on the feedback that was provided.

Proposal to approve the revised policy

34. Appendix A details the policy revision based on the feedback that was provided by agencies, including the RCOI Information Sharing Steering Group, and PSR Governance Group.
35. Appendix B details the current classification definition which have not changed.
36. Appendix C details the Glossary of terms used within the policy.
37. The Classification System policy 2022 (Appendix A) has been endorsed by the RCOI Information Sharing Steering Group and PSR Governance Group in January 2022.
38. We seek SIB's approval of the Classification System policy 2022 to commence from 1 July 2022.
39. Upon approval of the policy, the project can complete, test, and roll out the rest of the project deliverables between February and June 2022.

Recommendation

40. SIB is invited to:

a.	**Approve** the Classification System Policy 2022 (Appendix A).	**YES / NO**
b.	**Agree** The new policy will commence from 1 July 2022; However, transition and implementation is expected to take agencies 2 to 3 years with the first report back on progress in March 2023 and first measurement of performance in March 2024 (as part of their PSR annual assurance reporting).	**YES / NO**
c.	**Note** the concerns raised by agencies as part of the consultation and the responses on how their concerns would be addressed (Appendix D)	**YES / NO**
d.	**Note** the Classification definitions as agreed by Cabinet in 2000 have not changed (Appendix B)	**YES / NO**

e. **Note** The Director-General of NZSIS will socialise the policy and recommendations from SIB with the Minister for NZSIS and GCSB. **YES / NO**

Appendix A: Proposed Classification System Policy

Classification System policy 2022

The Government Information Security Classification System (Classification System) is owned and promoted by the Director-General of New Zealand Security Intelligence Service (NZSIS), which holds the Government's functional lead role as the Government Protective Security Lead (GPSL). Cabinet agreed to the Classification System in December 2000 [CAB(00)M42/4G(4)]. The Security and Intelligence Board (SIB) agreed to this policy on XX/XXX/XXXX.

This policy describes the Classification System -- New Zealand government's administrative system for the appropriate classification and handling of government information. It is not a statutory scheme but operates within the framework of domestic legislation.

Government information is all information, regardless of form or format, from documents through to data, that the New Zealand government collects, stores, processes, generates, or shares to deliver services and conduct business. This includes information from or exchanged with the public, external partners, contractors, or consultants and includes public records, email, metadata, and datasets.

Government information are key strategic assets that enable both short-term and long-term outcomes that benefit business, government, and the wider community and requires an appropriate degree of protection to keep it safe and available.

The purpose of the Classification System is to define how government information is classified to ensure it is appropriately used, managed, and protected. New Zealand government organisations and third parties who handle government information should consider their obligations to make available, manage, and protect government information. They do this under relevant legislation, cabinet directives, strategies and standards such as:

- Official Information Act 1982 (OIA)
- Local Government Official Information and Meetings Act 1987 (LGOIMA)
- Public Records Act 2005 (PRA)
- Privacy Act 2020 (Privacy)
- Public Service Act 2020 (PSA)
- Te Tiriti O Waitangi / The Treaty of Waitangi (Treaty)
- Declaration on Open and Transparent Government [CAB(11)29/12] (OTG)
- Information and Records Management Standard (IRMS)
- Protective Security Requirements [CAB (14) 39/38] (PSR).

There are two types of government information:

- Information that does not need increased security. This is called 'unclassified information and comprises most government information.
- Information that needs increased security measures to protect it from compromise.

Classification defines the sensitivity of the information (i.e. the likely harm that would result from its compromise) and defines the special handling and management needed to protect it. Note that classifications are a point-in-time risk assessment made by individuals. Classifications cannot of themselves be used to justify withholding information; rather any request for information must be considered on its merits using harm criteria defined within the relevant legislation.

This policy describes how New Zealand government classifies information and assets to:

- help New Zealand government appropriately share and use information to its full potential
- support New Zealand government to be open and transparent with the public
- protect information and assets appropriately
- meet the requirements of relevant legislation and international and bilateral agreements and obligations
- maintain the trust and confidence of New Zealanders.

The Classification System is mandatory for use within government departments, ministerial offices, the NZ Police, and the NZ Defence Force. This is aligned with the Cabinet decision in 2014 agreeing which agencies are mandated to follow the Protective Security Requirements (PSR) [CAB (14) 39/38].

The Classification System is made available for use by all other government organisations as a best practice policy framework for classifying, handling and protecting government information. These organisations are encouraged to voluntarily adopt the Classification System.

This Government Information Security Classification System Policy 2022 and supporting guidance will come into force on 1 July 2022 – until then, existing policy remains extant. Adoption of this policy by mandated agencies is expected to be completed within 2 to 3 years.

The Classification System policy principles

A foundational objective of the Classification System is to encourage and support **partnership and collaboration**.

The spirit of partnership and goodwill envisaged by Te Tiriti o Waitangi is encouraged and supported in how government information is made available, handled, shared and protected. People work together and are inclusive in the spirit of 'mahi tahi'. This principle contributes to learning, growth, and innovation of the Classification System to meet the ongoing needs of all New Zealanders.

The Classification System policy is based on these principles.

- **Organisational accountability**
- **Personal responsibility**
- **Information-sharing**
- **Information declassification**

Principle 1: Organisational accountability

New Zealand government agencies who handle government information must establish the conditions that enable people to handle government information correctly and safely.

Agency heads own their organisation's approach to classification and security, and invest in ongoing capability and improvement. The Classification System policy and principles are embedded within their organisation's policies and procedures and people are supported to encourage desired behaviour.

Policy to support organisational accountability

Policy Statement - Agency heads must establish an organisational classification policy and procedures in line with the Classification System and ensure that all people who handle government information do so correctly and safely.

The following requirements should be considered when establishing classification policies and procedures.

Resource and invest – Agency heads must own and maintain their organisation's approach to classification and security, and resource and invest in ongoing capability and improvement commensurate with the risks of information compromise that the organisation faces.

Obligations – Government information and assets must be handled in accordance with all relevant legislation, the Classification System, and regulatory requirements, including any international agreements and obligations. Agencies understand their obligations and build these requirements into the organisational classification policy and procedures.

Availability and transparency – Under legislation such as the Official Information Act 1982, Local Government Official Information and Meetings Act 1987, Privacy Act 2020, and Public Records Act (2005), agencies have an obligation to make government information available unless there is a good reason to withhold it. The relevant legislation sets the criteria for withholding information. Agencies must consider the public right to government information and define how they will meet these obligations within their organizational classification policies and procedures. This principle supports the core values of government transparency, accountability, and public participation. Information should be considered open, unless there is a compelling reason to withhold it.

Protection – Classification drives the appropriate security of the information. Classified information must be protected to ensure its availability, integrity, and confidentiality commensurate with its classification. Protection of classified information is controlled through appropriate personnel, physical, and information security mechanisms as defined within the PSR and NZISM.

Originator-controlled – The authority to classify or declassify rests with the originator and the organisation or government that controls the information. To ensure information is protected across its whole lifecycle, the originator and organisation or government that controls the information are responsible for establishing, communicating, reviewing, and managing how the information is handled by everyone with access to it. Agencies' classification policy and procedures must detail how originator control will be maintained over the information's lifecycle.

Partner information – Government information or assets received from or exchanged with external partners must be protected in accordance with legislative or regulatory requirements, including any international agreements and obligations. This policy applies equally to information entrusted to the New Zealand government by others, such as foreign governments, international organisations, NGOs, private organisations, and private individuals. Agencies' policy and procedures must detail the partner information security and management requirements and how these will be adhered to and monitored.

Education and training - Agency heads must provide their people with timely and ongoing classification training, assess their understanding and ensure that they have the ability to fulfil their government information obligations within the Classification System. This includes training on how to securely handle government information, including how to classify it, how to share it, and how to declassify it. This training should form part of the agency's wider information management and security training.

Regular reviews – Information sensitivity will change over the information lifecycle and the organisation's policy should prescribe when subsequent reviews of classification levels and protective markings are to take place for particular information types as part of their information and records management practices. The purpose of the review is to ensure that the protective markings were correctly applied initially and are still appropriate for the information as the information ages or changes. Outcomes of reviews should be tracked, reported and used as learning opportunities.

Measuring function and performance – In line with PSR GOV8 (Assess your capability), Agency heads must ensure that their organisation's classification capability and performance is assessed using the PSR Capability Maturity Model and annual PSR assurance process as part of their overall protective security programme.

Principle 2: Personal responsibility

Everyone who works in or with the New Zealand public sector, including employees, contractors, and suppliers, has a duty to classify, declassify and handle information appropriately. Individual classification, declassification, and sharing decisions are based on an effective risk assessment of the harm and impact of information compromise and in line with the organisation's classification system policies and procedures.

Policy to support personal responsibility

Policy Statement: Everyone must take responsibility to understand and fulfil their obligations to classify, declassify, and handle information correctly in line with the organisation's classification policy and legislative, regulatory, and other organisational obligations.

The following requirements should be considered when taking personal responsibility for classifying, declassifying, and handling government information.

Duty to safeguard – Individuals are responsible for protecting government information and assets in their care in line with their classification. Accidentally or deliberately compromising government information without authorization may lead to harm or damage and can be a criminal offence under relevant legislation (e.g. Crimes Act 1961, Criminal Disclosure Act 2008, Summary Offences Act 1981.)

Risk assessment – Individuals must make classification decisions based on the best information available. Decisions must be made transparently, based on a risk assessment that considers the level of harm and the likelihood of compromise.

Harm and impact – Individuals must assess and be able to articulate the level of harm and

impact that could eventuate to the organisation, individuals, government, or partners if the information or asset is compromised.

A considered approach – Information is of most value when it can be used appropriately by everyone who could benefit from its use. When assessing the harm of compromise, individuals should consider all audiences who could benefit from its use and look for ways to reach the widest audience to achieve the greatest benefit. When in doubt, individuals should consider whether the particularly sensitive information could be redacted or reframed at a lower classification level to achieve the greatest value of releasing or sharing the information for a specific audience.

Avoid over-classifying – Individuals must use classification appropriately. Over-classifying information causes serious harm, such as limiting access to necessary information, requiring infrastructure to store it and people to manage it, and increasing administration and cost to the New Zealand Government. Government information should only be classified when the result of compromise warrants the expense of increased protection. Government information must be classified and protectively marked at the lowest level possible that will still provide the necessary level of protection for its sensitivity.

Seeking and acting on learning opportunities – Accidental or unintended over- or under-classification will occur, and should be challenged and used as learning opportunities. People should be open to challenging others and being challenged themselves on classification decisions and security behaviours. Agencies should encourage a no blame culture that focuses on learning and improving classification and handling decisions over time.

Don't withhold information inappropriately – Individuals must not use classification to withhold information inappropriately. For example, government information should not be withheld to:

- hide violations of law, inefficiency, or administrative error
- prevent embarrassment to an individual, organisation, agency, or the government
- restrain competition
- prevent or delay the release of information that does not need protection in the public interest.

Principle 3: Information-sharing

Government organisations recognise that appropriately sharing decision-useful information with relevant organisations is a core foundation to protecting New Zealand and New Zealanders from threats, and for realising the potential of information to aid government effectiveness and enable wellbeing of New Zealanders. This is underpinned by a culture of trust between partners that shared information is handled and used appropriately and safely.

Policy to support information-sharing

Policy Statement: Agency heads must ensure that policies and procedures for handling classified information reinforce the value of information-sharing, collaboration, and cross-partner trust. They must implement effective and safe information-sharing practices within their agency and with other trusted partners. People are supported and empowered to achieve decision-useful sharing appropriately and safely.

The following requirements should be considered when establishing organisational information-sharing policies and procedures.

Stakeholders' needs – Agencies must understand the stakeholders they should share classified information with or collaborate with to achieve good stewardship of government information

and get the maximum benefit of the information for all New Zealanders. Agencies should look beyond their common information-sharing partners including other sector government organisations, international partners, local government, civil defence, hapū, iwi, and local communities. Agencies must work collaboratively to understand stakeholder needs and what decision-useful information-sharing looks like.

Legislative requirements – Agencies must understand their information-sharing obligations under relevant legislation (e.g. Privacy Act), and regulatory or partner agreements that enable and hinder information-sharing across partners.

Information flows and barriers – Agencies should understand how classified information flows between partners and identify any barriers to effective information-sharing. Where barriers exist, agencies should prioritise investment in removing those barriers where possible.

Use of information-sharing instruments – When appropriate, agencies should make appropriate use of available government information-sharing instruments (e.g. AISA, IMA, MoU). These instruments should include the criteria and rules for sharing between parties and any requirements for handling and declassifying classified information in compliance with their obligations.

Empowering information-sharing – Agencies must establish policies, procedures, and training for sharing classified information. This will give people confidence that they are complying with their obligations, contribute to increased trust in classified information-sharing, and empower people to share information appropriately, safely, and timely.

Principle 4: Information declassification

Government information must not remain classified indefinitely without being subject to review for declassification in line with the Public Records Act 2005, Information and Records Management Standard, and the organisation's declassification policy. This policy should be made available to the public to improve transparency and accountability of declassification decisions.

Policy to support information declassification

Policy Statement: Agency heads must establish an organisational declassification policy and procedures in line with the Classification System and relevant legislation including Official Information Act 1984, Public Records Act 2005, Privacy Act 2020, and requirements contained in relevant international agreements or arrangements.

The following requirements should be considered when establishing organisational declassification policies and procedures.

Understanding classified information holdings – To inform the design of their declassification policy and criteria, Agencies must have a clear understanding of their classified information holdings as part of their obligations under the Public Records Act 2005 and the Information and Records Management Standard.

Declassification policy – Agencies that hold classified information must have a policy that establishes a systematic approach to declassifying government information. This policy must prohibit the indefinite classification of government information without transparent criteria, review periods, and decisions. This policy should be made available to the public to improve transparency and accountability of declassification decisions.

Declassification criteria – Not all information may be suitable for declassification if it is of short-term or low value. Within the classification policy, decision makers need to set up and use criteria to clearly articulate the rules for declassification in the organisation (e.g. information

types, review periods, harm test rules, declassification topics and priorities). This criteria should be consistent with information and records management practices and decisions (e.g. appraisal, sentencing, and disposal.) The criteria should be used to prioritise how resources are allocated and to agree the scope and plan for a declassification programme. These criteria should be clear, transparent and objective and reflect the expected value to New Zealand of the declassification programme.

Declassification governance – Agencies must establish an appropriate governance framework for declassification. Governance must ensure that investment in declassification delivers value for the public, set precedents for reviews, arbitrate declassification decisions when conflicting opinions arise, and make final decisions on declassification matters that are referred for consideration.

Declassification programme – Agencies must appropriately resource and establish a regular programme for declassifying government information in line with their policy and priorities. Agencies must report transparently on the progress, results, and expected value that the programme delivered.

Appendix B: Classification definitions

Classifications are divided into two categories:

- Policy and privacy – classified to protect public interest or personal privacy.
- National security – classified to protect the security, defence, or international relations of New Zealand.

Policy and privacy classifications

The classifications for government information that should be protected because of public interest or personal privacy are:

IN CONFIDENCE

Use the IN CONFIDENCE classification when the compromise of information is likely to:

- prejudice the maintenance of law and order
- impede the effective conduct of government
- adversely affect the privacy of New Zealand citizens.

For instance, when the compromise of information could prejudice:

- citizens' commercial information
- obligations of confidence
- measures for protecting the health and safety of the public
- the substantial economic interest of New Zealand
- measures that prevent or mitigate material loss to members of the public.

Or when a compromise of information could:

- breach constitutional conventions
- impede the effective conduct of public affairs
- breach legal professional privilege
- impede the government's commercial activities
- result in the disclosure or use of government information for improper gain or advantage.

SENSITIVE

Use the SENSITIVE security classification when the compromise of information is likely to damage New Zealand's interests or endanger the safety of its citizens.

For instance, where compromise could:

- endanger the safety of any person
- seriously damage the economy of New Zealand by prematurely disclosing decisions to change or continue government economic or financial policies relating to:
    - exchange rates or the control of overseas exchange transactions
    - banking or credit regulations
    - taxation
    - the stability, control, and adjustment of prices of goods and services, rents, and other costs and rates of wages, salaries, and other incomes
    - the borrowing of money by the New Zealand Government
    - the entering into of overseas trade agreements
    - impede government negotiations (including commercial and industrial negotiations).

National security classifications

The classifications for government information that should be protected because of national security are:

RESTRICTED

Use the RESTRICTED security classification when the compromise of information would be likely to adversely affect the national interest.

For instance, where compromise could:

- adversely affect diplomatic relations
- hinder the operational effectiveness or security of New Zealand or friendly forces
- hinder the security of New Zealand forces or friendly forces
- adversely affect the internal stability or economic wellbeing of New Zealand or friendly countries.

CONFIDENTIAL

Use the CONFIDENTIAL security classification when the compromise of information would cause significant damage to the national interest.

For instance, where compromise could:

- greatly damage diplomatic relations and cause formal protest or other sanctions
- damage the operational effectiveness of New Zealand forces or friendly forces
- damage the security of New Zealand forces or friendly forces
- damage the effectiveness of valuable security or intelligence operations
- damage the internal stability of New Zealand or friendly countries
- disrupt significant national infrastructure.

SECRET

Use the SECRET security classification when the compromise of information would cause serious damage to the national interest.

For instance, where compromise could:

- raise international tension
- seriously damage relations with friendly governments
- seriously damage the security of New Zealand forces or friendly forces
- seriously damage the operational effectiveness of New Zealand forces or friendly forces
- seriously damage the effectiveness of valuable security or intelligence operations
- seriously damage the internal stability of New Zealand or friendly countries
- shut down or substantially disrupt significant national infrastructure.

TOP SECRET

Use the TOP SECRET security classification when the compromise of information would cause exceptionally grave damage to the national interest.

For instance, where compromise could:

- threaten the internal stability of New Zealand or friendly countries
- lead directly to widespread loss of life
- cause exceptional damage to the security of New Zealand or allies
- cause exceptional damage to the operational effectiveness of New Zealand forces or friendly forces
- cause exceptional damage to the continuing effectiveness of extremely valuable security or intelligence operations
- cause exceptional damage to relations with other governments
- cause severe long-term damage to significant national infrastructure.

Endorsement markings

ACCOUNTABLE MATERIAL	This marking shows that the information requires: • strict control over access and movement • regular auditing to ensure its safe custody (use a risk assessment to decide how often to audit). What constitutes ACCOUNTABLE MATERIAL will vary from agency to agency. Note: TOP SECRET information is ACCOUNTABLE MATERIAL by default
APPOINTMENTS	This marking may be used before you announce actual or potential appointments, or during the deliberation stage of a recommendation and approval process.
BUDGET	This marking may be used for proposed or actual measures for the Budget before their announcement.
CABINET	This marking may be used for material that will be presented to, and/or require decisions by Cabinet or Cabinet committees.
COMMERCIAL	This marking may be used for commercially sensitive processes, negotiations, or affairs.
[DEPARTMENT] USE ONLY	This marking may be used for material intended only for use within the specified department(s).
EMBARGOED	This marking may be used on material before a designated time at which an

FOR RELEASE	announcement or address will be made, or information will be disseminated.
EVALUATIVE	This marking may be used for material about competitive evaluations, such as interview records and tender assessments.
HONOURS	This marking may be used for material about the actual or potential award of an honour. It may be used: • before the announcement of the award • during the deliberation stage of a recommendation or approval process • when you are considering honours policy matters involving the exercise of the royal prerogative.
LEGAL PRIVILEGE	This marking may be used for material that is subject to legal privilege.
MEDICAL	This marking may be used for material relating to: • medical reports • medical records and other material related to them.
NEW ZEALAND EYES ONLY (NZEO)	This marking indicates that access to information is restricted to New Zealand citizens with an appropriate security clearance on a need-to-know basis.
STAFF	This marking may be used for material containing references to named or identifiable staff. It can also be used by staff for entrusting personal confidences to management.
POLICY	This marking may be used for material relating to proposals for new or changed government policy before publication.
TO BE REVIEWED ON	This marking may be used when the classification is to be reviewed at the designated time.
RELEASEABLE TO (REL TO)	This marking identifies information that is releasable to the countries or citizens of those indicated countries only.For example, RELEASABLE TO // NZL, GBR or REL TO // NZL, GBR means that the information may be passed to citizens and the governments of the United Kingdom and New Zealand only. Nation tri-graphs are: NZL, AUS, CAN, GBR, USA. Convention is for originating agency to be listed first, so NZL would be listed first, and the remainder in alphabetical order.

Appendix C: Glossary of terms

Term	Definition
Availability	Availability means that authorised users have access to the information that they need. See also Integrity and Confidentiality.
Classification System	New Zealand Government Information Security Classification System. This is New Zealand government's administrative system (principles, policies, guidance, tools, and resources) for the appropriate classification and handling of government information to ensure it is appropriately used, managed, and protected.
Classified information	Classified information is any government information that requires increased security and special handling to protect it. The information is generally protectively marked with the classification level (e.g. IN CONFIDENCE, SENSITIVE, RESTRICTED, CONFIDENTIAL, SECRET, TOP SECRET) and may also include other endorsement or compartmented markings. See also Protective marking, Endorsement marking, and Compartmented marking.
Compartmented marking	A compartmented marking is an additional protective marking that is combined with the classification and endorsement marking (if applicable) indicating that the information is in a specific need-to-know compartment. This word could be a codeword or 'Sensitive Compartmented Information (SCI)'. See also Protective marking, Need to know, Endorsement marking, and SCI.
Confidentiality	Confidentiality means that information is protected from unauthorised disclosure or access. See also Integrity and Availability.
Decision-useful information	Information is decision useful when it assists users to make good decisions or informs the development of advice to decision-makers. To be decision-useful, the information needs to be high-quality, timely, and accurate.
Declassification	Declassification is the process for reviewing the protective marking on information with the objective of removing classifications to facilitate the public release of information.
Endorsement marking	An endorsement marking is an additional protective marking that combined with the classification, warn people that information has special handling requirements. The endorsement marking may indicate the specific nature of information, temporary sensitivities, limitations on availability, or conditions for handling. See also Protective marking and compartmented marking.
Government information	Government information is all information, regardless of form or format, from documents through to data, that the New Zealand government collects, stores, processes, generates, or shares to deliver services and conduct business. This includes information from or exchanged with the public, external partners, contractors, or consultants and includes public records, email, metadata, and datasets.
GPSL	The Government Protective Security Lead (GPSL) is a leadership role appointed by the Public Service Commissioner to the Director-General of the New Zealand Security Intelligence Service (NZSIS).
Information compromise	Information compromise is the accidental or unauthorised loss, disclosure, removal, tampering, or misuse of the information.
Integrity	Integrity means that information is protected from unauthorised changes to ensure it remains reliable and correct. See also Availability and Confidentiality.

Term	Definition
NZISM	New Zealand Information Security Manual. The Government's manual on information assurance and information system security.
Open information	Open information is unclassified information that has been made available to the public for their use and sharing. See also Unclassified information.
Partners	Partners refer to all individuals, groups, organisations, or governments where information is shared.
Privacy	A person's ability to control the availability of information about them.
Protective marking	Protective marking is the practice of marking the information with its classification, endorsement markings, and compartmented markings (if applicable) such as within paragraphs, emails, documents, metadata, or systems to inform readers and users of their obligations for securely handling and protecting the information.
PSR	Protective Security Requirements (PSR) outlines the Government's requirements for managing personnel, physical, and information security. The Classification System is a core foundation to the PSR. The PSR was approved by Cabinet in 2014 [CAB (14) 39/38]
SCI	Sensitive Compartmented Information. Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Intelligence Community. See also Compartmented marking, Need to know.
Security	The controls and measures that an organisation uses to protect their people, information and assets.
Unclassified information	Unclassified information is any government information that doesn't need increased security or therefore does not require classification or protective marking. Most government information fits this category. It is optional for agencies to use a protective marking on unclassified information (e.g. UNCLASSIFIED) to clearly show that the information does not require any special handling.

Appendix D: Agency Feedback Themes

The following table summarises the feedback themes from agencies and defines what the project has done to address the feedback.

Ref.	Theme	Project Response
F1	Implementation may require centralised support, funding and resources.	The project will deliver standard education and other resources to make it easier for agencies to adopt the policy. The project will also provide guidance on how to implement and manage the change in their environment. The PSR team will be provided with support and training including a train-the-trainer package to enable the team to support agencies to undertake the work after the project closes. A multi-agency community of practice could be stood up to provide targeted support if required. A number of agencies have expressed interest in participating in a community. As part of the agency's protective security annual improvement plan and capability maturity assessment, they should assess and plan the classification programme change and if required seek additional funding and resources to undertake the programme.
F2	Is this change a priority for Government?	The priority for this work was set by the RCOI who recommended that this change be completed within six months. The Government accepted the recommendations in principle. Although we will not meet the prescribed time limit by the RCOI, it signals the intended level of priority they ascribed to completing this work. Each agency should agree the priority for this work with their responsible Minister and in consultation with the Lead Coordination Minister for the Government's Response to RCOI.
F3	This policy and RCOI and IGIS are asking for an all-of-government approach to classification and security but the current agency mandates do not support this.	Acknowledged. The PSR team are currently working on a separate initiative to review the mandate for the PSR and Classification System to be more future proofed and based on an assessment of the protective security risks that an organisation or sector poses to the national security of New Zealand or to the well-being of New Zealanders.

Ref.	Theme	Project Response
F4	The policy supports RCOI 9a and 9b but is not sufficient in itself to achieve the desired outcomes. Systemic issues and barriers exist that prevent good classification practice, declassification, and information sharing.	Acknowledged. This policy establishes the foundational conditions and sets the expectations for the desired behaviours for good classification practice. The project will also provide standard resources that agencies can use to achieve to standardise practice in their environment and achieve the policy objectives. Agencies will need to assess how they will achieve the policy objectives and encourage the desired behaviours within their environment. Where barriers or issues exist that will prevent the agency from achieving the intent, they will need to prioritise investment and resources required to remove or mitigate the barriers where possible. Other RCOI initiatives are in progress or are planned to address systemic issues preventing effective information sharing (e.g. people's security clearance levels, technology security and compatibility, or infrastructure / physical site access.)
F5	Without simplification of the Classification System, we may not achieve the desired objectives. It will be a waste of effort to implement this change and then do it over again when the System is simplified.	Acknowledged. Simplification is out of scope for this project. Additional funding is being sought to continue the classification system simplification work. Although simplification will make it easier to achieve the overall objectives set by RCOI and make it easier to get classification right, it does not negate the need for standard education and practice on classification. This project will deliver updated classification, information sharing, declassification, and performance measurement guidance, standard tools and resources, and education and training packages that agencies can use and tailor to their specific environment. Even if the Classification System is simplified, older information will remain marked with previous classification levels as reclassifying or declassifying all historical information is not feasible or appropriate. Knowledge and education on the previous classification system policy will still be needed for years after the change occurs. If approved to be delivered, the simplification project would build upon and extend the resources developed by this project including how to map between the old and new Classification System requirements.

Ref.	Theme	Project Response
F6	'Need-to-know' is not well understood and is inconsistent with the Information Sharing principle and may prevent effective information sharing.	In the classification system / PSR information security guidance we will clarify the definition of 'need to-know' and how and when it should be applied. We will work with Reference Agencies to agree this practice and guidance, The practice for 'need to know' is often applied too generally and used as a basis for not sharing information. The Information Sharing principle establishes requirements for agencies to understand who they need to share information with, identify the barriers that prevent information sharing with them, and to seek to eliminate barriers where possible. Culture change around the 'need-to-know' may be one of those barriers that needs to change within an agency. With the Organisational Accountability principle, each agency should define in their classification policy and procedures how their organisation applies the 'need-to-know', for which roles and types of information, why it is required (based on the risk posed by its compromise) and how the need-to-know is managed. This will provide clarity to all on which information can and cannot be shared and with whom because the 'need-to-know' applies. See also Compartmented marking.
F7	The policy needs to be simplified, terms defined and standardised, and statements focused on the specific action/requirement for the audience.	Acknowledged. We have made changes to the policy to address this feedback: • Added a Glossary of Terms and standardised on the use of those terms. • Removed content that was informational which will move into guidance. • Removed two of the principles (Education and Training, and Governing Performance) as there was overlap and some duplication with Organisational Accountability and Personal Responsibility principles. • Reframed some of the requirements statements to be clear on the specific action required by agencies or individuals.
F8	The policy has limited relevance to non-mandated agencies or those who only work with IN CONFIDENCE or SENSITIVE classification levels.	The policy applies equally to all classified information at any level from IN CONFIDENCE through to TOP SECRET. Although the RCOI and IGIS emphasised information sharing and declassification for highly classified information, the concepts also apply to information sharing and declassification at lower classification levels. We acknowledge that some classification concepts and practices primarily apply to highly classified information (e.g. compartmented marking, SCI, 'need-to-know'). Guidance will be tailored to enable agencies to apply the principles and requirements when they hold information only at lower classification levels (e.g. IN CONFIDENCE, SENSITIVE, or RESTRICTED).

Ref.	Theme	Project Response
F9	Is the intent for declassification programmes to target all levels of classification or only highly classified government information (e.g. CONFIDENTIAL, SECRET, TOP SECRET)? What is the value of declassification for agencies who hold only SENSITIVE or IN CONFIDENCE information?	Declassification occurs across all classification levels. All agencies already have requirements to declassify and make available government information in line with relevant legislation (e.g. OIA, PRA, Privacy.) In particular, this will occur in line with PRA requirements for information appraisal, sentencing, and disposal processes. We acknowledge that the declassification programme within agencies with highly classified information will look differently to those in agencies with SENSITIVE or lower information. Declassification guidance will be provided or referenced to existing legislative guidance to assist agencies in declassifying classified information at any level on both an ongoing and historical basis. The guidance will also address the practice required relating to government information received from other organisations or governments. Declassification policies and programmes within an agency should be commensurate with their classified information sets, requirements for and priorities for declassification as set by the organisation's leaders and Minister, their need for greater openness and transparency, and the resources available in the organisation to achieve it.

<table>
<tr><th>Ref.</th><th>Theme</th><th>Project Response</th></tr>
<tr><td>F10</td><td>Effective measurement is based on central government establishing a simple and standard set of indicators that all agencies could use. How will performance of the system be measured and tracked?

Will there be time limits for when agencies must meet the classification policy requirements?</td><td>The project will establish the standard set of indicators that all agencies will use. Minor updates are being made to the PSR Capability Maturity Model, PSR Self-assessment and reporting, and PSR moderation framework to include the new indicators. Agencies will not require changes to their technology systems to measure performance. Guidance will be provided to agencies on how to measure and report on their capability as part of their annual PSR assurance processes.

There will not be defined time limits for when agencies must fully meet the policy requirements. However, agencies must report back on the status of their classification programmes and assess their capability maturity based on the new performance indicators in their March 2024 PSR assurance report. Below is an example of the timeframes and likely activities that agencies should plan to undertake:

<table><tr><td>July 2022 – March 2023</td><td>April 2023 – March 2024</td></tr><tr><td>Assess requirements for undertaking a classification programme. Plan and agree how this can be achieved. Request and obtain additional funding if required.

If possible, begin classification programme.

Report back on the planning and status of their classification programme in March 2023 PSR assurance report.</td><td>Start or continue the classification programme.

First measurement of classification performance in March 2024 PSR assurance report.</td></tr></table></td></tr>
<tr><td>F11</td><td>The narrative suggests that the NZIC will provide system governance. It is unclear how this will work, who leads, and how it interacts with existing system level governance (e.g. Archives NZ, Ombudsman, Privacy Commissioner). With a limited mandate, is system level governance actually possible?</td><td>Acknowledged. With the current functional leadership role, the GPSL is not responsible for governing all government organisations' application of the policy. As is the case with the PSR, it is each agency's accountability to decide and govern its protective security and classification system capability development and improvement based on the risks it faces. The GPSL (and the PSR function) provides oversight of New Zealand government protective security through the PSR assurance process for mandated agencies. GPSL can only be responsible for ensuring that the Classification System remains fit for purpose and use by all organisations who use it and provide leadership, guidance and support to agencies in its use

The policy was updated to reflect this feedback.</td></tr>
</table>

Appendix E: Agencies who participated in consultation

The following agencies responded to our request for feedback between October 2021 and January 2022.

Antarctica New Zealand
Crown Law Office
Department of Conservation
Department of Corrections
Department of Internal Affairs (including Archives New Zealand)
Department of Prime Minister and Cabinet
Government Communications Security Bureau
Inland Revenue Department
Maritime New Zealand
Ministry for Culture and Heritage
Ministry for Pacific Peoples
Ministry for Primary Industries
Ministry for the Environment
Ministry of Business, Innovation and Employment
Ministry of Defence
Ministry of Education
Ministry of Foreign Affairs and Trade
Ministry of Health
Ministry of Justice
Ministry of Social Development
New Zealand Customs Service
New Zealand Defence Force
New Zealand Police
New Zealand Security and Intelligence Service
Office of the Ombudsmen
Oranga Tamariki – Ministry for Children
Parliamentary Service
Privacy Commissioner
Public Service Commission
Reserve Bank of New Zealand
Serious Fraud Office
Statistics New Zealand
The Treasury
Waka Kotahi - NZ Transport Agency