Office of the Inspector-General of Intelligence and Security

A review of the New Zealand Security Classification System

Report

Cheryl Gwyn
Inspector-General of Intelligence and Security
August 2018

Contents

PURPOSE, SCOPE AND APPROACH

i. The purpose of this review is to identify changes that could be made to the New Zealand security classification system to improve security, reduce costs and increase transparency. The terms of reference, which were self-generated, are attached as Appendix 1.

ii. The security classification system operates across government, while my statutory remit is limited to oversight of the New Zealand Security Intelligence Service (NZSIS) and the Government Communications Security Bureau (GCSB or 'the Bureau'). To that extent the review reaches beyond the usual scope of activity for my Office. I have undertaken it, however, with agency support, as a voluntary independent contribution to an agency-led review of government personnel security requirements.

iii. The approach I have taken presumes that any change to New Zealand's security classification system would be made through the usual government policy process, involving consultation with affected agencies. I sought and was grateful to receive some information from agencies both within and outside the intelligence sector.[1] I do not pretend, however, to offer a thorough assessment of the likely costs and benefits of change to a system used by multiple agencies, each with its particular needs and operational constraints. Instead I have sought to put forward ideas and analysis that provide a starting point and a cogent direction for change.

[1] I am grateful for assistance from officials of NZSIS, GCSB, DPMC, NAB, MFAT, Police, Customs, the Defence Force, the Cabinet Office and Archives New Zealand.

1: THE NEW ZEALAND SECURITY CLASSIFICATION SYSTEM

Introduction

1. Security classification exists to identify official information that needs special management to avoid risks that would arise if it was freely accessible. The system protects such information by controlling access to it, through a combination of protective markings, associated rules and procedures (eg handling requirements and rules restricting access to security cleared personnel) and physical or technical barriers (eg locked storage, encryption).

2. The primary classifications are categories of information, defined according to the level of risk of harm that might arise from open access to the information. Each classification is accompanied by rules about the security required around the information when it is stored and transmitted. Information is assigned a classification according to its risk and labelled (usually) with the corresponding protective marking.

3. Although "classification" in its broadest sense identifies the system for controlling access to official information, it has a more specific meaning within the system. A classification is a specific type of protective marking, identifying the level of sensitivity attaching to information. In the New Zealand system, TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED, SENSITIVE and IN CONFIDENCE are classifications.[2]

4. Other markings used with classifications to indicate specific controls on access, the sensitivity of a source, or the nature of the information are not themselves classifications. When used with a classification, however, they add to its meaning. The 'classification' of that information will usually then be understood as encompassing the full set of controls applying to it, arising from its actual classification plus other markings.

5. Security clearance rules define classes of people who *may* have access to the information in each classification category. Whether they actually do have access generally depends on whether those who can establish and enforce controls on access are satisfied that those seeking access have a 'need to know'.

6. A classification system exists to preserve the value of official information so that the public interest in retaining and using it can be realised. At the lower end of security, this might mean protecting personal information that agencies have been allowed to collect for the purpose of providing public services. At the higher end it might mean protecting intelligence that gives an advantage to national decision-makers. At every level the purpose is to protect information so it can be used to the best effect. Classification must limit access to the extent necessary for protection, but enable access to the extent necessary to realise its value and justify the effort and intrusion involved in acquiring it. Secrecy has no value for its own sake: its only purpose is to ensure that information is used as it should be.

---

[2] This report follows the practice common among agencies that use classifications of capitalising classification descriptors. So, for example, "CONFIDENTIAL information" refers to information classified CONFIDENTIAL, while "confidential information" refers to information to which a legal obligation of confidence attaches.

Law

7. Classification is not mandated or required by any statute. It is an administrative act, done within a legal framework that provides public rights of access to official information and emphasises the democratic value of open government. The foundational statute in this framework is the Official Information Act 1982 (OIA).

Official information Act 1982

8. The OIA is:

> An Act to make official information more freely available, to provide for proper access by each person to official information relating to that person, to protect official information to the extent consistent with the public interest and the preservation of personal privacy, to establish procedures for the achievement of those purposes, and to repeal the Official Secrets Act 1951.[3]

9. Under the OIA "official information" is any information held by the New Zealand Government and its agencies, including the intelligence and security agencies.[4] Official information is not limited to material stored digitally or in writing or in any other format, but can include anything known to an agency, including in the memory of an employee.[5]

10. Under section 5 of the OIA all official information is subject to the principle of availability:

> 5 Principle of availability
>
> The question whether any official information is to be made available, where that question arises under this Act, shall be determined, except where this Act otherwise expressly requires, in accordance with the purposes of this Act and the principle that the information shall be made available unless there is good reason for withholding it.

11. The OIA identifies grounds for withholding official information when access to it is sought by a member of the public. Among the possible "conclusive" reasons for withholding is that making the information available would be likely to "prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand."[6] The Act also empowers the Prime Minister to veto the release of official information on national security grounds.[7]

12. Information may also be withheld under the OIA for reasons including the protection of privacy, an obligation of confidence, public health and safety or New Zealand's economic interests. These reasons are not conclusive, but may justify withholding information unless the reasons

---

3 Long title.
4 See section 2 definitions of "official information" and "organisation".
5 "Guide: The OIA for Ministers and agencies" Office of the Ombudsman (June 2016) at 6.
6 Section 6(a).
7 Section 31.

for doing so are outweighed by considerations which render it desirable, in the public interest, to make the information available.[8]

13. A classification marking is only indicative of whether there is any public right of access to the information under the OIA. At the highest levels of classification, if they have been correctly applied and the reasons remain relevant, it will be likely that conclusive reasons to withhold exist. At the lower levels of classification (again if correctly applied) it will be merely possible that conclusive reasons to withhold exist. For most material at low classifications there will be, at most, good reasons to withhold. Whatever the classification, it is not decisive: the availability of information under the OIA must be assessed on its merits at the time.

Privacy Act 1993

14. The Privacy Act controls how government agencies collect, use, disclose, store and give access to personal information. It sets out 12 privacy principles that generally apply to government agencies.

15. The NZSIS and the GCSB are subject to all privacy principles except three relating to collection of personal information.[9] In effect this exemption frees the agencies to collect personal information on people from sources other than the people themselves, and to collect it in ways that might otherwise be unacceptably intrusive or unfair.

16. Under the Privacy Act people are entitled to request from a government agency, including the NZSIS and the GCSB, any personal information the agency holds on them. A request can be refused on the grounds (among others) that disclosure would be likely to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand.[10]

17. In practice the intelligence and security agencies may release personal information in response to requests, confirm that they do not hold any, or 'neither confirm nor deny' that they hold any information. Requesters can complain to the Privacy Commissioner if they are not satisfied with the agency's response.

Public Records Act 2005

18. The Public Records Act 2005 requires every public office, which includes the intelligence and security agencies,[11] to create and maintain full and accurate records of its affairs.[12] Records under the Act differ from official information under the Official Information Act in that they comprise information that has been compiled, recorded, or stored in written form or on some other medium.[13]

19. Once they have been in existence for 25 years, records must be transferred to the national archives unless certain exceptions apply. These include an exception for any records that a

---

8 Section 9.
9 Principles 2, 3 and 4(b): see section 315 of the Intelligence and Security Act 2017.
10 Section s 27(a).
11 Section 4.
12 Section 17.
13 Section 4.

responsible Minister certifies as containing information whose release would be likely to prejudice national security, defence or international relations, or prejudice the entrusting of information to the Government on a basis of confidence by another government.[14]

20. An agency can keep historic records, rather than transfer them to Archives, under a 'deferred deposit' agreement. To do so it must certify that it needs to retain the records for its business and undertake to store and protect them appropriately.

21. Records transferred to the Archives can be classified as 'restricted access,' with the terms of the restriction determined by the head of the relevant agency in consultation with the Chief Archivist.[15] Archives prefers however to receive records without access restrictions. Its storage security also falls short of the standards for storage of classified information. Most historic classified records consequently remain in secure storage administered by GCSB.

Intelligence and Security Act 2017

22. The Intelligence and Security Act 2017 (ISA) governs the NZSIS, the GCSB and their oversight.

23. The Act defines "security records" broadly, effectively capturing all information received or generated by the agencies in the course of their business.[16] Security records are official information, which has the same meaning in the Act as in the OIA 1982.[17]

24. The ISA does not mandate classification, but establishes offences and penalties for improper disclosure of information.[18] It also addresses the classification of IGIS inquiry reports.[19]

Crime statutes

25. The Crimes Act 1961 and Summary Offences Act 1981 state some offences in relation to official information. The Crimes Act defines offences of espionage, wrongful communication or copying of classified or official information and sabotage.[20] The Summary Offences Act defines an offence of unauthorised disclosure of certain official information.[21]

Policy

The Protective Security Requirements

26. The security classification system is applied under the authority of Cabinet. The decision endorsing the system now in use dates from December 2000.[22]

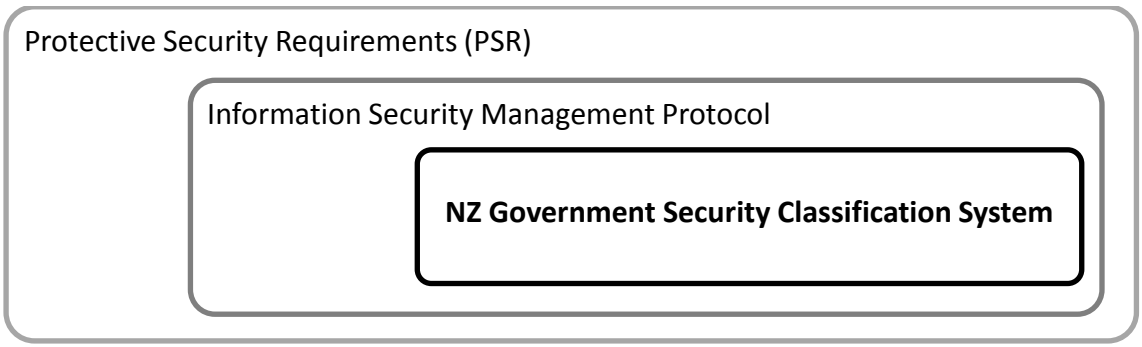
27. The primary source of policy on classification is the Protective Security Requirements (PSR), approved by Cabinet in December 2014.[23] The PSR is a set of policies on security governance,

---

14 Section 22(6).
15 Section 44(3).
16 Section 4.
17 See s 4 definition of "official information".
18 See for example sections 108, 109, 219.
19 Section 185.
20 Sections 78, 78A, 78AA, 79.
21 Section 20A.
22 CAB(00)M42/4G(4).
23 CAB Min 14 39/38.

personnel security, information security and physical security. It sets out a mixture of mandatory requirements and recommended practices.

28. One of the mandatory requirements for information security is that agencies must implement policies and protocols for the protective marking and handling of information in accordance with the PSR, New Zealand Government Security Classification System (GSCS), and the New Zealand Information Security Manual.[24] The GSCS is a policy within the Information Security Management Protocol of the PSR:



'Need to know'

29. The PSR identifies the 'need to know' principle as "the fundamental rule of personnel security" applying to government agencies.

30. The guidance in the PSR is that before granting access to information, "agencies should establish the existence of a legitimate need to access protectively marked resources to carry out official duties."[25] Although this limits application of 'need to know' to protectively marked (classified) information, the GSCS says it applies to all official information:

> To reduce the risk of unauthorised disclosure, agencies must take all reasonable and appropriate precautions to ensure that only individuals with a proven 'need-to-know' are granted access to official information, regardless of whether it is subject to the security classification system or not.[26]

31. The Information Security Manual states that access to TOP SECRET information systems must only be granted on a 'need to know' basis. For all other systems 'must' becomes 'should'.[27]

32. In principle, 'need to know' is a broader control on officials' access to official information than classification. It applies to unclassified official information and can limit access to classified information for officials who otherwise have sufficient security clearance to receive it.

---

[24] INFOSEC4, Strategic Security Objectives, Core Policies and the Mandatory Requirements for Agencies.
[25] At 4.3.
[26] At 2.
[27] At 9.2.6.

33. ‘Need to know’ is formalised within the classification system by compartmentalising classified information. This is the use of markings and/or technical barriers to restrict access to sub-groups among those that have general access to information with the relevant classification.

34. It is curious, on the face of it, that a government official should only have access to official information on the basis of a need to know, when a member of the public seeking access to the same information under the OIA might be entitled to it without having to establish any such need. Government employees can however be seen as custodians of official information that the public has allowed them to collect. Officials may access this information to the extent necessary to perform their functions, subject to a constant duty of justification. A general, qualified public right of access to official information serves as a check on the legitimacy of government collection and use of information. This is the public ‘need to know’.

Classification principles

Some official information is ‘national security information’

35. The classification system divides official information into two fundamental categories: information that does not need increased security and information that does.[28] A vast range of official information is unprotected and freely accessible in reports and other publications, on websites and so on.

36. Protected information is in turn divided into two categories: national security information and everything else. The GSCS defines national security information as:

> … any official information or resource, including equipment that records information about or is associated with New Zealand's:
>
> - protection from espionage, sabotage, politically-motivated violence, promotion of communal violence, attacks on New Zealand's defence system, acts of foreign interference and the protection of New Zealand's territorial and border integrity from serious threats
> - defence plans and operations
> - international relations, significant political and economic relations with international organisations and foreign governments
> - law enforcement operations where compromise could hamper or make useless national crime prevention strategies or particular investigations or adversely affect personal safety
> - national interest that relates to economic, scientific or technological matters vital to New Zealand's stability and integrity.[29]

37. The GSCS notes that not all national security information needs to be protectively marked: it should only have a national security classification if its compromise or misuse could damage

---

28 GSCS at 2.

29 At 3.4.

national security, the Government, commercial entities or members of the public.[30] Identifying official information as national security information is therefore only an administrative convenience – a preliminary step towards determining what, if any, protective marking might be required.

38. Official information that requires protection, but not for reasons of national security, can relate to the safety or privacy of individuals; private commercial interests; legal processes; and government finances, negotiations, policy development, or transactions. Protection can also be required where the use of information is subject to privilege, obligations of confidence or constitutional conventions.

Classification is based on risk assessment

39. The basis in principle for applying a security classification to official information is an assessment of the risk of harm if the information was to be made generally available.

40. The lowest levels of classification, covering official information that is not relevant to national security, are known as policy and privacy classifications. The risks to be considered when deciding whether to apply these classifications are whether free availability of the information would:

- prejudice the maintenance of law and order, impede the effective conduct of government in New Zealand, or adversely affect the privacy of New Zealand citizens (classification: IN CONFIDENCE); or
- damage the interest of New Zealand, or endanger the safety of New Zealand citizens (classification: SENSITIVE).

41. For the higher levels of classification — national security classifications — the assessment is of risk to "national interests". Classifications apply with an increasing level of protection according to whether free availability of the information would:

- be likely to affect the national interests in an adverse manner (RESTRICTED)
- damage national interests in a significant manner (CONFIDENTIAL)
- damage national interest in a serious manner (SECRET)
- damage national interest in an exceptionally grave manner (TOP SECRET).[31]

42. The GSCS identifies Business Impact Levels as a tool for assessing the risks associated with compromise of sensitive official information:

> Official information needing increased protection is identified by considering the Business Impact Levels (BILs) of its unauthorised disclosure by compromise or misuse.... Where an assessment of business impact levels indicates compromise or misuse of information would have adverse results,

---

30 At 3.4.

31 See Annex A to the GSCS.

> that information must be given extra protection in line with the severity of the damage resulting from such compromise. It must be protectively marked.[32]

43. Cross-referenced information on Business Impact Levels does not however constitute further guidance on classification. It notes that:

> At times there *may* be a relationship between security classification of official information and BILs.... A protective marking alone does not determine the impact level, nor does the impact level alone determine the protective marking.[33] [Emphasis added.]

44. An annexe to the BIL guidance sets out criteria for identifying BILs from 1 (low) to 6 (catastrophic). The BIL guidance maps the 'likely' relationship between BIL levels and classifications.

45. BILs appear to function primarily as a tool for assessing the protection required for official information at a system or database level. They are not a routine reference for decisions about protective marking.

Aggregation of information can increase risk

46. The PSR advises that the aggregation of official information "can mean the overall classification of a collection needs to be higher than the classification(s) of its individual elements."[34] Specific guidance is that aggregations such as databases can be protected by more stringent access controls without increasing the classification of the whole, but:

> A discrete collection of information may be assessed as requiring a higher protective marking where the aggregated information is significantly more valuable, because it reveals new and/or more sensitive information or intelligence than would be apparent from the individual data sources. Examples could include data collections that support intelligence assessments or are designed to show evidence of fraud.[35]

47. Applying a higher classification to the aggregation would not however change the protective marking of any of the component data.[36]

Authority to classify belongs with the originator

48. Classification systems typically distinguish between:

- original classification: decisions about the classification of newly acquired or created information; and

---

32 INFOSEC4, Strategic Security Objectives, Core Policies and the Mandatory Requirements for Agencies at 4.
33 Business Impact Levels at 2.1.
34 Information Security Protocol at 5.4.
35 Management of Aggregated Information at 2.5.
36 Management of Aggregated Information at 2.5.

- derivative classification: decisions made about the classification of material that includes or incorporates information that has already been classified.

49. Most classification is derivative. In the United States, where executive branch agencies are required to provide data on classification activity, they reported just under 40,000 original classification decisions in 2015-16 and just over 55 million derivative classification decisions.[37]

50. Classification systems commonly operate on the principle that the original author or compiler of information is in the best position to assess the risks that might arise from unfettered access to it. Any subsequent use of the information should therefore defer to the classification determined by that person or their agency.

51. The PSR refers to an original classifier as an 'originator'. It sets no limits on who may be an originator, such as a minimum level of seniority or experience. Instead it states that an agency protective marking guide (which is mandatory) should cover who can apply protective markings. It notes that some agencies require a senior officer to confirm the application of protective markings above a certain level, including the use of endorsement and/or compartmented markings.[38] The GSCS advises that agencies "should have a procedure for confirming protective markings, especially where such a marking is not normal or standard for that agency."[39]

52. Procedures for derivative classification are also supposed to be included in agency protective marking guides, subject to the principle of originator control. The PSR advises that derivative classification procedures "should include marking information at the same level or higher than that received and how to request permission to use part of the information at a lower level."[40]

53. Classified information received from another government should in principle have its protective marking determined by the New Zealand official "actioning" it, according to the GSCS, and markings suggested by outside organisations or individuals should not automatically be accepted unless by prior agreement.[41] Agency protective marking guides should cover the marking of information received from foreign governments, in accordance with any relevant agreements. Comparative tables of protective markings are encouraged.[42]

54. The principle of originator control also applies to changing a classification. A derivative classifier who considers a classification inappropriate may query it with the original classifier but not change it without their agreement. This holds at both the individual and the agency level.[43]

<u>Official information should be classified no more than necessary</u>

55. The GSCS is clear that as little official information as possible should be classified:

---

37 Information Security Oversight Office, Annual Report 2016 at 1.
38 Developing Agency Protective Security Policies, Plans and Procedures at 4.2
39 At 4.3.
40 Developing Agency Protective Security Policies, Plans and Procedures at 4.2
41 At 4.2.
42 Developing Agency Protective Security Policies, Plans and Procedures at [4.2]
43 At 4.4 and 4.8.

> New Zealand government holdings of protectively marked information should be kept to a minimum.[44]

56. It also expressly recognises over-classification as a risk:

> Official information should only be protectively marked when the result of compromise warrants the expense of increased protection.
>
> It is important that official information not requiring protection remains UNCLASSIFIED.
>
> Inappropriate over-classification has many seriously harmful effects:
>
> - public access to government information becomes unnecessarily limited
> - unnecessary administrative arrangements are set up that will remain in force for the life of the document, including repository arrangements for information transferred to Archives New Zealand, imposing an unnecessary cost on the agency
> - the volume of protectively marked information becomes too large for an agency to protect adequately
> - the New Zealand Government Security Classification System and associated security procedures are brought into disrepute if the protective marking of official information is unwarranted. This may lead to protective markings being devalued or ignored by agency employees or receiving agencies.
>
> For these reasons, the New Zealand government expects that agencies will only protectively mark information when there is a clear and justifiable need to do so. [45]

57. Minimising classification means minimising duration as well as volume. The GSCS states that agencies should limit the duration of protective marking, including by trying to set a specific date or event for declassification based on how long the information will remain sensitive.[46]

<u>Classification must not be used for improper purposes</u>

58. The GSCS states that:

> Under the Official Information Act 1982, official information must not be protectively marked to:
>
> - hide violations of law, inefficiency, or administrative error

---

44 At 4.
45 At 4.5.
46 At 4.5.

- 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.[47]

59. This does not derive from the wording of the OIA, but as a statement of classification policy it has appeared in United States Executive Orders on classification, with minor variations, since 1972.[48] In New Zealand guidance it dates at least to 1983, when it was included in a government handbook on security in government departments and organisations.[49]

Protective markings

60. The GSCS defines the protective markings to be used for official information and the criteria for their application. Agency policies on protective marking are required by the PSR to provide "detailed guidance to identify agency-generated information that requires a protective marking".[50]

61. Security classification markings are divided into two categories: policy and privacy markings; and national security markings. Although all are classifications, within government only material with a national security marking is commonly referred to as "classified".

Policy and privacy markings

62. The policy and privacy security classifications are IN CONFIDENCE and SENSITIVE, with sensitive being the higher classification. The GSCS defines them as follows:

IN CONFIDENCE

The IN CONFIDENCE security classification should be used when the compromise of information would be likely to prejudice the maintenance of law and order, impede the effective conduct of government in New Zealand or affect adversely the privacy of its citizens.

For instance, where compromise could:

- prejudice the maintenance of law
- adversely affect the privacy of natural persons
- prejudice citizens' commercial information
- prejudice [an] obligation of confidence
- prejudice measures protecting the health and safety of members of the public
- prejudice the substantial economic interest of New Zealand
- prejudice measures that prevent or mitigate material loss to members of the public
- breach constitutional conventions
- impede the effective conduct of public affairs
- breach legal professional privilege
- impede government commercial activities

47 At 4.
48 Executive Order No. 11652 (8 March 1972).
49 State Services Commission, Security in Government Departments and Organisations: A Handbook for Staff (August 1983).
50 Developing Agency Protective Security Policies, Plans and Procedures at 4.2.

- result in the disclosure or use of official information for improper gain or advantage.

SENSITIVE

The SENSITIVE security classification should be used when the compromise of information would be likely to damage the interest of New Zealand 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
    - the regulation of banking or credit
    - 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).

63. The criteria for the policy and privacy classifications are close replicas of OIA criteria for withholding official information. The IN CONFIDENCE criteria almost all correlate with good reasons for withholding information under section 9 of the OIA.[51] The SENSITIVE criteria almost all correlate with conclusive reasons for withholding information under section 6 of the OIA.[52]

National security markings

64. The national security classifications are, in ascending order of sensitivity: RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET. The GCSC criteria for these are:

RESTRICTED

The RESTRICTED security classification should be used when the compromise of information would be likely to affect the national interests in an adverse manner. For instance, where compromise could:

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

[51] The exception is compromise to the maintenance of the law, which can be a conclusive reason to withhold under section 6 of the OIA.

[52] The exception is impeding government negotiations (including commercial and industrial), which can be a good reason to withhold under section 9 of the OIA.

CONFIDENTIAL

The CONFIDENTIAL security classification should be used when the compromise of information would damage national interests in a significant manner. For instance, where compromise could:

- materially 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

The SECRET security classification should be used when the compromise of information would damage national interest in a serious manner. 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

The TOP SECRET security classification should be used when the compromise of information would damage national interest in an exceptionally grave manner.
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.

65. The criteria for the national security classifications predominantly relate to one conclusive reason for withholding official information under the OIA: to avoid prejudice to national security or international relations.[53] They may also relate to avoiding prejudice to the entrusting of information to the Government by other governments and international organisations, which can also be a conclusive reason to withhold.[54]

Compartmented markings and endorsement markings

66. Compartmented markings are not security classifications but may be added to material that has a security classification. The GSCS describes them as indicating that the information "is in a specific need-to-know compartment."[55] The markings may be generic codewords attaching to

[53] See section 6(a).
[54] See section 6(b).
[55] At 3.7.

particular types of information (eg COMINT, for signals intelligence), or codenames for access groups. Typically people must be briefed on the sensitivities of the information in a compartment before they will be given access.

67. Endorsement markings can also be added to a security classification. They indicate that the information has special requirements in addition to those indicated by the classification. Endorsement markings commonly used on national security classified material include NEW ZEALAND EYES ONLY (NZEO) and RELEASEABLE TO (REL TO). Endorsement markings commonly used on policy and privacy classified material include BUDGET, CABINET, COMMERCIAL and LEGAL PRIVILEGE.

'Unclassified'

68. Most official information does not meet the threshold for a security classification. It is generally referred to as 'unclassified' information and may be marked as such, but need not be. Officials and agencies that deal mostly with unclassified information tend not to label it. The 'unclassified' marking is applied mostly within agencies that primarily deal with classified material, to avoid uncertainty.

Declassification and downgrading

69. Under the PSR agencies are expected to set up classification review procedures. This includes reviewing the protective marking of information regularly, "for example, after a project or sequence of events is completed or when a file is withdrawn from or returned to use."[56] Protective marking review procedures should be included in an agency's protective marking guide.[57]

70. Classified information “should be declassified as soon as it no longer meets the criteria for protective marking,” according to the PSR, and agencies should have a declassification programme.[58]

71. The principle of originator control applies, so that any proposed change to classification must be agreed by the original classifier or classifying agency.[59]

Access control

72. Access control mechanisms are applied to some extent across all official information, including classified. Broadly they enable or limit access to information based on ‘need to know’.

73. Access control can be implemented through basic administrative decisions information (eg on who is copied into email or included in meetings); use of software-based access restrictions in IT systems (eg the allocation of read, write and edit privileges on electronic documents); physical barriers around records and systems (eg safes, building access controls); and compartmented markings or dissemination controls (or both) on classified material.

---

56 GSCS at 4.7.
57 Developing Agency Protective Security Policies, Plans and Procedures at 4.2.
58 Information Security Management Protocol at 5.6.
59 GSCS at 4.7.

74. Agencies holding sensitive information in higher security systems will usually have a stronger 'perimeter' around the data, restricting access to staff who have a level of security clearance that exceeds a basic pre-employment check, logging and auditing access and using access controls such as two-factor authentication. Within these systems there may be compartments of data accessible only to an authorised subset of staff. Compartmented digital information can be made invisible to unauthorised users: the system will not just deny them access, it will give them no indication the information exists.

75. The intelligence sector, in response to heightened concerns about 'insider threat' following the disclosure of classified material by Edward Snowden and others, has adopted and continues to develop "attribute based access control." Both information and users are tagged with metadata that is compared to determine whether access is authorised. Essentially this aims to eliminate anonymous access to protected information. All interactions with information are logged. Logs can be audited to detect suspicious activity or determine culpability for leaks.

Storage, handling and disposal requirements

76. Each level of classification has associated requirements for storage, handling and disposal of information and media. The level of security required increases as the classification rises.

77. For information on paper, storage requirements begin with being kept in a building with the normal level of security applied to a government office (for IN CONFIDENCE). Anything SENSITIVE and above must be kept in lockable storage, with increasing requirements for the security of the container and the building as the classification increases. Requirements for transmission of paper documents escalate similarly. Material up to RESTRICTED can be sent by commercial courier, subject to specific enveloping requirements. Material classified CONFIDENTIAL and above must be transferred by safe hand, or diplomatic bag if moving internationally.[60] Disposal requirements are at departmental discretion for IN CONFIDENCE then escalate up to supervised, highly specified destruction methods for highly classified material.

78. For electronic documents and data, the critical distinction is between material that may be stored and transmitted on internet-facing systems and material that may not. Information up to and including RESTRICTED is in the first category: it can be kept and exchanged between agency systems that are not isolated from the internet ('low side' systems), subject to the use of low grade encryption for anything SENSITIVE or RESTRICTED. Anything CONFIDENTIAL and above can only be stored and transmitted on non-internet-facing 'high side' systems and networks, using high grade encryption.[61] Disposal requirements also increase sharply in rigour between RESTRICTED and CONFIDENTIAL.

Security clearances

79. A person must have a national security clearance (through vetting by NZSIS) to have access to information classified at CONFIDENTIAL and above. A national security clearance is not required

[60] In exceptional circumstances CONFIDENTIAL material can be sent by registered mail.

[61] High side systems can in fact be connected to the internet through intermediate systems and one-way diodes, but their essential function is prevent access from or to the internet.

for access to material up to RESTRICTED, although employees with access to such material are still subject to pre-employment screening.

80. There are four levels of national security clearance; CONFIDENTIAL, SECRET, TOP SECRET and TOP SECRET SPECIAL. A CONFIDENTIAL clearance will be granted if nothing adverse is found. The higher clearances involve increasingly extensive inquiries into the candidate and increasingly positive assessments of the candidate's trustworthiness, honesty and loyalty to New Zealand.

81. Agencies are supposed to determine the level of clearance an employee needs based on their 'need to know': the extent to which they need access to classified material or systems to do their job.[62] In an emergency or other exceptional circumstances a person may be given temporary, supervised access to material one level up from their normal level of access, but this cannot be granted to systems and information classified CONFIDENTIAL and above.

Agency policies and procedures

82. I reviewed a small selection of agency policies on classification. Some simply reproduce the GSCS criteria for applying classifications. Others provide additional guidance, by giving agency-specific examples of information that would meet the different classification thresholds.

83. The policies I saw generally do not limit authority to classify. One exception is the New Zealand Defence Force, where the minimum rank required to apply a classification rises with the level of classification.

84. Agency procedures for dealing with successful OIA and privacy requests provide for ad hoc declassification. Procedures for systematic declassification are more variable.

85. The most extensive and longstanding systematic declassification programme is run by the Ministry of Foreign Affairs and Trade (MFAT), which has been reviewing historic files for downgrading or declassification since the early 1990s. About 90 percent of reviewed files are declassified, with most of the remainder being given an end date for restricted access.

86. The Defence Force has been systematically reviewing old records since late 2009. It has declassified and transferred to Archives about 3600 files and other records, dating between 1936 and 2005.

87. The NZSIS began a limited programme of systematic declassification of historical records in 2008. Under an authorisation from the Chief Archivist the Service does not routinely transfer any historic classified records to Archives.[63] It has one staff member reviewing historic files resulting in the release of a small number of files per year.

88. The GCSB does not yet have a systematic declassification programme, but is developing a broader framework for management of its records that will enable one.

---

62 PSR "National Security Clearance Levels: Guidance for Agencies".

63 Under s 22(1)(d) of the Public Records Act 2005.

Interoperability with other systems

89. Intelligence and security agencies within the Five Eyes alliance[64] routinely share intelligence but have different classification systems. They therefore need agreed arrangements for the treatment of each other's classified material. The lead in establishing these arrangements is taken by the USA, whose Office of the Director of National Intelligence (ODNI) publishes comparison tables of protective markings.[65]

90. In principle the ingestion of one country's classified material into the classification system of another country does not result in the material being re-classified: the classification remains that applied by the originating country. The recipient country handles the material as if it had the appropriate classification within its own system, to ensure it is handled with no lesser level of security.

91. Differences in classification systems – mostly at the lower levels – produce some asymmetry in the way classifications compare (see Appendix 2). This arises because where one country does not have a marking that corresponds directly to the marking of information received, it will protect that information to a higher rather than a lower level. So, for example:

- US material marked UNCLASSIFIED: FOR OFFICIAL USE ONLY will be handled by New Zealand as RESTRICTED
- Australian material with the dissemination control markings Sensitive or Official Use Only will be handled by New Zealand as SENSITIVE
- New Zealand material marked RESTRICTED will be handled by Canada as CONFIDENTIAL
- New Zealand material marked CONFIDENTIAL will be handled by Britain as SECRET
- British material marked OFFICIAL-SENSITIVE will be handled by NZ as RESTRICTED.

92. Some New Zealand classification is driven by partner country requirements that access to certain systems or equipment will be restricted to people with a specific level of security clearance. Some weapons systems and other defence technologies, for example, are supplied to New Zealand on condition that they are operated only by personnel who have passed a 'negative' vet, which corresponds to a CONFIDENTIAL clearance and classification.

Statistics on classification

93. The terms of reference for this review included seeking empirical measures of the performance of the classification system.

94. The main international example I have found of an attempt to compile meaningful statistics on classification is provided by the United States. The Information Security Oversight Office (ISOO) reports annual tallies of:

---

64 The members of the alliance are the United States, United Kingdom, Canada, Australia and New Zealand.

65 The tables are an appendix to the Intelligence Community Markings System Register and Manual.

- original classification authorities (people with authority to classify)
- original classification decisions (and how many of these are applied for 10 years or less) and
- derivative classification decisions (estimated)
- formal challenges to classifications and their outcomes.

95. The ISOO also reports statistics on declassification processes, including the number of pages of information reviewed and declassified as a result of requests, systematic declassification and automatic declassification. It provides estimated total costs of the security classification system.

96. ISOO data is compiled from self-reporting by agencies. The Office acknowledges that estimates of derivative classification decisions – by far the dominant source of classified material – are problematic for agencies to generate and the Office to analyse.[66] Some observers question the reliability of the data more broadly.[67]

97. New Zealand agencies generating classified information are not required to report comparable statistics on classification activity and do not do so.

98. The GCSB was able to provide me with approximate measures of hard copy records held by Intelligence Community agencies in secure storage.[68] These total just under 2500 linear metres. The Bureau also provided statistics on data in its electronic document management system, which show the steady growth that would be expected in any government agency. The Bureau holds much larger volumes of intercepted data (some of it temporarily) in separate repositories.

99. I did not attempt to extract and compile further statistics from agencies on their holdings of classified information. I decided this would not be illuminating unless it was possible to analyse trends over time and that such a project was beyond the resources of this review.

100. I note however that there is no apparent issue – for the intelligence agencies at least – with capacity to continue generating and storing classified information. Secure storage space for hard copy records that are in regular use is limited, but secure archival storage space is ample. For electronic information, where the main growth now occurs, the cost of increasing storage is relatively low compared to the sunk costs of establishing highly protected systems and the ongoing cost of keeping them secure. (Up to a point: as storage increases, system architecture can become increasingly strained and require new investment, eg in restructuring repositories and reconfiguring relationships between them).

---

66 ISOO Annual Report 2016 at ii.

67 See eg Steven Aftergood "Amount of Classification is Highly Uncertain" (11 October 2016) Secrecy News <fas.org>.

68 The records belong to GCSB, NZSIS, DPMC (including NAB), Defence and MFAT.

2: CLASSIFICATION REFORM

101. This part of my report summarises the history of the New Zealand classification system, then surveys changes that have been made or proposed to other nations' systems. For ease of comparison the changes made in other countries are grouped under the themes of simplification, self-inspection, authority to classify, declassification and oversight.

102. The overseas focus is on New Zealand's 'Five Eyes' partner countries. This is due mainly to the greater accessibility of information about their systems. By far the most substantial source of open source information and analysis is the United States.

103. Partner countries' classification systems are also of particular interest, however, because New Zealand regularly exchanges classified information with them. There are also similarities in the statutory frameworks covering official information.

Drivers for reform

104. The prompts for classification reform in New Zealand and other countries have included major shifts in the security environment (eg the end of the Cold War), changes in public policy on official information (eg the OIA in New Zealand, the Freedom of Information Act in the US) and reviews of significant leaks of sensitive information. Reviews have also been initiated from general concern to ensure classification systems remain fit for purpose.

105. Many reforms have been directed at making classification decisions more accurate and consistent. This includes by avoiding under-classification, to ensure information is properly protected.

106. Avoiding or at least reducing over-classification is however a more prominent theme, as classification systems have an inherent bias toward over-classification. This bias has been exhaustively analysed – particularly in the US – and is widely recognised. Most official classification guides acknowledge the risk of over-classification and warn against it. The essential problem is that security bureaucracies give officials powerful reasons to over-classify and little or no reason to avoid or challenge over-classification. There are rarely if ever any adverse consequences for an official who is 'too careful.' Being – or being seen as – not careful enough can however mean professional disaster. Nor are there rewards, or generally much satisfaction, in challenging the classification decisions of others.

107. Over-classification has several harmful effects. By impeding the effective sharing of information it can contribute to intelligence failures. Public funds are wasted in providing unnecessarily high levels of protection for unnecessarily large volumes of material. Demand for security clearances is increased, with resulting additional expense and delay. Public access to official information, including the historical record, is excessively restricted. And the effectiveness of classification is undermined as officials who frequently encounter over-classified material lose respect for the system.

Reform in New Zealand

108. In New Zealand until the 1980s official information was managed on the principle that it should not be disclosed without specific reason or authority. Classifications applied additional restrictions, typically to defence, diplomatic, intelligence and Cabinet material. In 1983 the Official Information Act 1982 (OIA) entered into force and the Official Secrets Act 1951 was repealed. The OIA reversed the restrictive presumption governing access to official information, replacing it with the principle of availability.

109. The classification system was revised in conjunction with the new legislation. Since 1951 the markings TOP SECRET, SECRET, CONFIDENTIAL and RESTRICTED had been in use. Cabinet agreed in 1982[69] to issue a directive on security classification reducing the grades of classification to three: TOP SECRET, SECRET and CONFIDENTIAL, with revised criteria.[70]

110. In reforming classification the government was following the recommendations of the Committee on Official Information (usually known as the Danks Committee, after its chairman). The Committee recommended narrowing the scope for classification. It had found that the small number of departments that classified extensively tended to classify too highly.[71] It also took issue with classification criteria that resulted in classification on grounds other than national security. It was inappropriate, for example, that information could be classified CONFIDENTIAL if it might cause "administrative embarrassment, or difficulty", or prejudice to "any governmental activity."

111. The Danks Committee recommended dispensing with the RESTRICTED classification because it had "never been related to substantial national security concerns." At the time RESTRICTED could be applied to any information "which for security reasons should not be published or communicated to anyone except for official purposes."[72] The Committee also recommended provision for systematic review of all classified papers originating from 1976 onwards, for declassification, and declassification of older records as part of their processing for transfer to the National Archives.[73]

112. The three-level classification system lasted until late 2000, when Cabinet agreed to reintroduce the RESTRICTED classification. At the same time it authorised the new policy and privacy classifications of SENSITIVE and IN CONFIDENCE.[74] The Cabinet paper proposing the changes[75] argued that the new classifications would remedy deficiencies in the three-level system:

- The SENSITIVE and IN CONFIDENCE classifications would enable appropriate protection for information requiring protection for reasons other than national

---

69 Cabinet Directive on Security Classification CO (82) 14 (17 December 1982) reproduced in *Security in Government Departments and Organisations: A Handbook for Staff* State Services Commission (August 1983).

70 See Appendix 3.

71 Committee on Official Information *Towards Open Government (1) General Report* (December 1980) at [86].

72 Committee on Official Information *Towards Open Government (2) Supplementary Report* (July 1981) at [5.06].

73 Committee on Official Information, *Towards Open Government (2) Supplementary Report* (July 1981) at 5.17.

74 Cabinet Minute "Protection of Official Information" (18 December 2000) CAB (00) M 42/4G(4).

75 Cabinet Paper "Protection of Official Information" (8 December 2000) EXG (00) 124.

security, such as preserving personal privacy and avoiding premature disclosure of government decision-making.[76]

- The RESTRICTED classification would reduce over-classification of material as CONFIDENTIAL that occurred merely because there was no lower classification available. This was resulting in large volumes of information being unnecessarily processed in systems using high-grade encryption, particularly within the overseas cable system of MFAT. Introducing RESTRICTED would also harmonise the New Zealand system better with those of its overseas partners, particularly Australia. Australia supplied agencies such as MFAT and NZDF with information classified RESTRICTED that had to be upgraded in New Zealand to CONFIDENTIAL.[77]

113. The Cabinet paper discussed the options of extending the national security classification system to cover all information requiring protection; introducing a separate framework for protecting information not relating to national security; and bringing national security, policy and privacy classifications into a single unified system (as in the UK). It noted that these options were considered at length by an Interdepartmental Committee on Security and through consultation with relevant government departments. The preferred option was to have separate frameworks for national security and non-national security information, on the grounds that:

- Using national security classifications for all information needing protection would be "inflexible" and would impose excessive protective security requirements on administrative information, particularly material held in electronic form;[78]

- A single unified system mixing national security concerns with other reasons for protecting information would lead to a "somewhat inflexible system, with a tendency toward over-protection of information and unnecessary costs."[79]

- Having separate frameworks would "avoid any potential for conflict between the very specific requirements of the national security environment and the risk management approach that is more relevant for protecting other types of official information."[80]

114. The revised classification system was applied to Cabinet documents from August 2001 and Departments were briefed on the new requirements. The *Security in the Government Sector* manual was revised and republished online in 2002.

115. In 2006, following a disclosure of commercially sensitive Cabinet material, DPMC commissioned an independent review of its systems and practices in relation to the handling and security of sensitive information.[81] The review terms of reference included considering the adequacy of

---

76 At [3].
77 At [8].
78 At [9].
79 At [11].
80 At [10].
81 David Henry Review of DPMC systems and practices in relation to the security of sensitive information (23 June 2006).

the classification system for protecting highly sensitive Cabinet papers of a public policy nature (ie not dealing with matters of national security).

116. The reviewer recommended the introduction of a third policy and privacy classification, "Highly Sensitive," for Cabinet material requiring more protection than the SENSITIVE classification.[82] Papers on particularly sensitive matters were being marked with the endorsement "Personal to" the minister, but the related handling restrictions were inconsistently observed within ministerial offices. Requiring papers to be handled only by the addressee could also be troublesome for ministers.

117. Rather than introduce a further classification, Cabinet agreed on officials' advice in 2007 to introduce a new handling endorsement, SPECIAL HANDLING REQUIRED, which can be used with the SENSITIVE classification. It should be applied if compromise of the information would be likely to seriously and substantially damage national finances or economic and commercial interests; seriously impede the effective conduct of government; or seriously endanger the safety of any person.[83]

118. In December 2014, following a review of government protective security arrangements, Cabinet adopted the PSR as a replacement for the *Security in the Government Sector* (SIGS) manual.[84] The version of the GSCS incorporated in the PSR replaced that in the SIGS manual.

119. Some small changes to classification policy resulted from the adoption of the PSR:

    119.1. The PSR relaxed the policy on who could classify information and encouraged agencies to develop their own guidelines. The 2002 SIGS manual stated that "Chief Executives and heads of government departments and agencies, State Owned Enterprises and Crown Entities are vested with the authority to classify material using the approved classifications. Chief Executives may delegate authority to classify to senior staff, but sparingly. In particular, only appropriate senior staff should be given authority to classify material SECRET or TOP SECRET. It is important to avoid unwarranted application of these classifications by less experienced staff."[85] The PSR guidance is that "the person or agency responsible for preparing information or for actioning information produced outside the New Zealand government is to decide its protective marking" and that "Agencies should have a procedure for confirming protective markings, especially where such a marking is not normal or standard for that agency."[86]

    119.2. The PSR replaced advice in the SIGS manual on "downgrading classifications"[87] with much briefer advice that agencies should review protective marking regularly.[88] The PSR advice is arguably for the most part just a more concise expression of the SIGS manual advice,

---

82 Henry, recommendation 5.1.

83 Department of the Prime Minister and Cabinet "Introduction of SPECIAL HANDLING REQUIRED Endorsement" (19 May 2011).

84 CAB Min 14 39/38.

85 Department of Prime Minister and Cabinet *Security in the Government Sector* (2002) at 3-4 [17]-[18].

86 New Zealand Government Security Classification System at 4.1 and 4.3.

87 At 3-6 [30]-[33].

88 New Zealand Government Security Classification System at 4.7.

apart from the shift in emphasis away from "downgrading" classification to the more neutral "review".

120. The major changes to the New Zealand classification system are summarised in the timeline attached as Appendix 4.

Reform in other countries

Simplification

Australia

121. In 2011 the Australian government revised its security classification system, cutting the number of classifications from seven to four. The changes followed a two-year review of protective security policy that found support across the Federal government for simplifying the system.

122. Before the changes, 'national security information' (defence, security and diplomatic) was classified as TOP SECRET, SECRET, CONFIDENTIAL or RESTRICTED. Non-national security information (any other sensitive official information requiring special protection, eg commercial and personal) was classified as HIGHLY PROTECTED, PROTECTED or X-IN-CONFIDENCE ('X' being a placeholder for a subject matter label such as STAFF, SECURITY, COMMERCIAL or AUDIT). Cabinet material was marked 'Cabinet-in-Confidence' but protected and handled, at a minimum, as PROTECTED.[89]

123. The 2011 reform abolished the HIGHLY PROTECTED, RESTRICTED and IN-CONFIDENCE classifications. Classified information in Australia is now TOP SECRET, SECRET, CONFIDENTIAL or PROTECTED:

Australian classification system changes, 2011

Former national security classification →	**New classification**	← Former non-national security classification
TOP SECRET	**TOP SECRET**	
SECRET	**SECRET**	HIGHLY PROTECTED
CONFIDENTIAL	**CONFIDENTIAL**	
	PROTECTED	PROTECTED
RESTRICTED	For Official Use Only (FOUO)*	X-IN-CONFIDENCE
* FOUO is a dissemination control rather than a classification		

124. The dissemination control marking "For Official Use Only" (FOUO) was introduced for information with the potential to cause limited damage to national security, government agencies, commercial entities or members of the public if released. There are four other

[89] The Auditor-General *Operation of the Classification System for Protecting Sensitive Information* (Australian National Audit Office, 1999) at Appendix 1.

dissemination control markings ("Dissemination Limiting Markers" in the Australian terminology):

> Sensitive - for use on classified and unclassified documents
>
> Sensitive: Cabinet - used with PROTECTED as a minimum classification
>
> Sensitive: Legal - for use on classified and unclassified documents
>
> Sensitive: Personal - for use on classified and unclassified documents[90]

125. Routine official information that does not require protection may be marked UNCLASSIFIED, but need not be.

126. The classification system continued to recognise a distinction between national security information and other information that might require classification.[91] The definition of national security information was later replaced by a broader definition of "national interest" information.[92]

127. A more recent review of Australia's protective security policy found that 'UNCLASSIFIED' and the new Dissemination Limiting Markers (FOUO, Sensitive) were often misunderstood and misapplied. In response officials are considering replacing UNCLASSIFIED with 'OFFICIAL' and replacing FOUO; Sensitive; Sensitive: Legal; and Sensitive: Personal with a single marking of OFFICIAL-Sensitive. Ministers may be asked for decisions at the end of 2017.

United Kingdom

128. In 2014 the UK undertook the most radical simplification of classification adopted amongst New Zealand's intelligence partners. A multi-layer scheme of classifications from TOP SECRET to UNCLASSIFIED was reduced to three tiers: TOP SECRET, SECRET and OFFICIAL.[93]

129. The old system was seen as "complex, costly and burdensome," developed for a system of paper records predating modern electronic document systems and email. It was also held to be poorly understood, particularly at the lower levels, and commonly misapplied. The UK Government decided the system need to be made "more straightforward and intuitive, and the associated security controls more demonstrably effective and proportionate." The new scheme was expected to be easier to comply with, resulting in more consistent classification, better protection of sensitive information and better use of information technology. [94]

130. The issues with the old system were described more colloquially by the Cabinet Office minister who oversaw the changes, who was reported as saying that security restrictions on his Cabinet

---

90 "National Security Information Environment Roadmap: 2020 Vision; *How To Guide*" Australian Government Department of the Prime Minister and Cabinet (2012) Attachment A at 14.

91 Australian Government Information security management guidelines: Australian Government security classification system (18 July 2011: Version 1.0) at 3.11.

92 "National interest information" includes any "official resource", including equipment, that concerns national security; international relations; law and governance; economic, scientific or technological matters; heritage or culture -- Australian Government *Information security management guidelines: Australian Government security classification system* (November 2014: Version 2.2) at 3.11.

93 Cabinet Office (UK) "Government Security Classifications" (April 2014).

94 Cabinet Office (UK) "FAQ: International Classification Policy" (August 2013) at [2] and [5].

Office computer made it so cumbersome to use that he "nearly threw it out of the window." He had given up trying and would only deal with secret information on paper. He noted that documents marked RESTRICTED, although accessible to thousands of officials within the department holding them, could not be emailed outside the department.[95]

131. The table below shows how the new UK classifications relate to the old.

UK Classification System changes, 2014

Old classification		New classification
TOP SECRET	No direct mapping between classifications	TOP SECRET
SECRET		
CONFIDENTIAL		SECRET
RESTRICTED		
PROTECT		OFFICIAL
UNCLASSIFIED		

132. Material marked OFFICIAL can have the caveat SENSITIVE attached, which brings additional handling requirements. The descriptors COMMERCIAL, PERSONAL or LOCSEN (for sensitive information that locally engaged overseas staff cannot access) can be attached to classifications, as can codewords (usually only to SECRET and TOP SECRET) and national 'eyes only' caveats.[96]

133. The new classifications do not directly map to the old, although guidance material explains that:

- material that would have been classified TOP SECRET or SECRET would generally remain at least SECRET
- formerly CONFIDENTIAL material could become SECRET or OFFICIAL-SENSITIVE;
- material up to and including RESTRICTED would generally become OFFICIAL.[97]

134. The OFFICIAL classification was expected to be sufficient for the vast majority of public sector information. It applied personnel, physical and information security controls based on commercial good practice.[98] For OFFICIAL information, departments were expected to be able to replace expensive, bespoke information systems with more flexible and cheaper commercially available systems.[99] Guidance material noted that the review leading to the

---

95 Oliver Wright "The secret's out: Whitehall's document classification system devised to thwart German spies in WWII is finally being streamlined" *The Independent* (United Kingdom, 16 October 2013).

96 Cabinet Office (UK) above n 94 at 11-12.

97 Cabinet Office (UK) "Government Security Classifications FAQ Sheet 1: Working with OFFICIAL Information" (April 2013) at 2.

98 Cabinet Office (UK), above n 98 at 1.

99 Comptroller and Auditor General *Protecting Information Across Government* (National Audit Office, UK, 14 September 2016) at [2.25].

introduction of the new system had found instances of material over-classified at CONFIDENTIAL, indicating that some CONFIDENTIAL material could also become OFFICIAL.[100]

135. A key change to guidance was the direction to classifiers to consider distinctly the two factors of (i) impact if the information is compromised and (ii) the level of threat. Information was only to be classified at the highest levels (TOP SECRET or SECRET) if both the consequences of compromise were sufficiently serious (in the terms set out for each classification) and the information required defence against "highly capable, determined and well resource threat actors (in essence hostile foreign intelligence services or high-end organised crime groups)."[101]

136. The new approach emphasises the need to avoid over-classification. Guidance material advises:

> Organisations must be mindful that there is a very significant step up (a cliff face) from OFFICIAL to SECRET, and that the benefits of the new policy will be eroded if they are too risk averse and seek to put more information into SECRET than is absolutely necessary.[102]

137. The removal of UNCLASSIFIED means all UK government information is OFFICIAL, as a minimum, whether it is so marked or not. Guidance material is clear that there is no presumption that OFFICIAL information will be widely accessible: "there is no presumption of disclosure or unbounded access at any level of the classification policy."[103] The first principles of the UK classification system are that all official information "has intrinsic value and requires an appropriate degree of protection" and that everyone who works with government, including contractors and service providers "has a duty of confidentiality and responsibility to safeguard any HMG information or data that they access, irrespective of whether it is marked or not."[104]

138. The UK classification regime applies not only within the national security sector but to all central government, police, health services, local and regional government. Suppliers of goods and services to the public sector are also expected to classify and handle appropriately any information relating to their dealings with government. [105]

139. The UK system provides for use of Business Impact Levels (BIL) — which were already in use — for information risk assessment. A Fujitsu UK analysis of the new system suggested that an impact level could be derived from a protective marking, "but it is definitely not safe to do so the other way" – ie an appropriate classification could not necessarily be determined by assessing the business impact of release.[106]

140. The UK guidance is clear that aggregation, while it might increase the potential impact of loss, compromise or misuse, does not of itself justify a higher classification.[107] A large holding of OFFICIAL records is not to be classified SECRET as a result of its size. Instead, aggregated data

---

100 Cabinet Office (UK), above n 98 at 2.
101 Cabinet Office (UK), above n 98 at 2.
102 Cabinet Office (UK), above n 98 at 2.
103 Cabinet Office (UK), above n 98 at 2.
104 Cabinet Office (UK), above n 94 at [1] and [5].
105 See https://www.gov.uk/government/publications/government-security-classifications
106 Fujitsu UK "An Interpretation of the new Government Security Classification Scheme" (March 2014).
107 Cabinet Office (UK), above n 94 at [32].

sets are to be "carefully and tightly controlled, eg by avoiding aggregation at rest on end user devices."[108]

141. Implementing the UK reforms has apparently had its difficulties. In September 2016 the UK National Audit Office reported that despite more than two years of policy development and communications, departments were poorly prepared for implementation of the revised classification system:

> Many have seen the benefits of implementing the new system, but some still have concerns about their ability to protect information. There is considerable confusion about how to use the classification system properly and misunderstanding about the requirements for securely transmitting and storing information classified as Official outside government networks, including the use of cloud and encryption services.[109]

142. The Audit Office found that this confusion resulted in significantly different handling of OFFICIAL information by departments. Some treated it as they formerly would have handled UNCLASSIFIED information, moving it freely across the internet and using personal email accounts. Others insisted on sending it only between encrypted departmental accounts.[110] Some departments regarded OFFICIAL-SENSITIVE as an indicator only of enhanced handling requirements for information that remained OFFICIAL. Others regarded OFFICIAL-SENSITIVE as a higher classification.[111]

143. The Audit Office also reported that it was not always straightforward to align classifications under the simplified classification system with protective markings used by other organisations. Although the Cabinet Office had provided guidance, adoption of good practice remained "patchy". Staff could look for equivalent definitions, leading to additional markings that undermined the simplicity of the system:

> The result is that there is no common understanding of each classification, nor agreed handling protocols. This potentially undermines each classification's security status as it moves between – and is reinterpreted by – staff in different departments.[112]

144. The business case for the revised classification system had not been based on achieving financial savings, the Audit Office reported, although annual savings of £110-£150 million had been estimated. A detailed financial business case had been proposed but never completed, so the Cabinet Office was unable to say what financial benefits had been realised.[113]

United States

145. The military classifications of RESTRICTED, CONFIDENTIAL and SECRET used by the United States during the Second World War were expanded in 1950 by the addition of TOP SECRET, to align

---

[108] Cabinet Office (UK), above n 94 at [32].
[109] Comptroller and Auditor General, above n 100 at [2.27].
[110] At [2.28].
[111] At [2.29].
[112] At [2.30].
[113] At [2.31]-[2.32].

the US system with those of its allies. In 1953 the RESTRICTED classification level was eliminated. The primary security classifications have been TOP SECRET, SECRET and CONFIDENTIAL ever since. Material that is not security classified may be marked FOR OFFICIAL USE ONLY (FOUO), but this is not a national security classification.

146. Despite having only three levels the US national security classification system has often been criticised as unduly complex and there is a substantial literature of reform proposals. The complexity lies not at the basic classification level but in the use of a wide range of secondary control markings. Many of these are created by agencies for their own purposes. Often they are used without a security classification, creating confusion about what classification means.

147. In 1994, for example, the US Joint Security Commission noted that on top of the three fundamental classification levels there were at least nine additional categories of controls applied by major agencies, with multiple levels in each category. These were generally systems of compartmented access control. The Department of Defense had more than 100 'Special Access Programs', many with numerous compartments and sub-compartments. The Commission was told that the system was out of control, with administrators of special access programmes effectively able to set their own rules.[114] It responded by proposing a radical simplification of the US classification system:

> Under this system, information either is classified or it is not. There would be a single legal definition of classified information and no need to pretend that we can precisely measure the amount of damage to national security that would be caused by an unauthorized disclosure.[115]

148. The Commission's system would have had a single classification of SECRET, but with provision for a subset of SECRET material to be designated SECRET COMPARTMENTED ACCESS. This would be subject to higher security protection standards, require a higher level of security clearance for access and be subject to need-to-know access lists. It would incorporate most information held as TOP SECRET and subject to compartmented access.[116] Although some of the Commission's other recommendations were implemented, its proposal for simplifying classification was not.

149. Nor was a simplification proposal in 2012 from the Public Interest Declassification Board, a body established by Congress to advise the President. The Board essentially recommended merging CONFIDENTIAL and SECRET into a single classification, leaving the system with just two levels, SECRET and TOP SECRET.[117]

150. In 2010 an effort began to impose order on a welter of quasi-classifications used for non-national security information.[118] In the US lexicon, information that is subject to access, distribution and handling controls for reasons such as privacy, commercial sensitivity and law enforcement sensitivity is not 'classified', but 'controlled unclassified information' (CUI). The programme is intended to reform and standardise more than 100 different agency-specific

---

114 United States Joint Security Commission "Redefining Security" (February 1994) Chapter 2 at 3.
115 Joint Security Commission, above n 122 at 3.
116 Joint Security Commission, above n 122 at 5-6.
117 Public Interest Declassification Board "Transforming the Security Classification System" (November 2012).
118 See <www.archives.gov/cui>.

policies and procedures. The ISOO, which is managing the programme, has reported progress,[119] but it has also reportedly run into opposition from agencies.[120]

151. The failure to date of proposals for simplification means that changes to the US system have generally been around authority to classify and, particularly, declassification processes (both covered below).

152. In March 2016, however, former Director of National Intelligence James Clapper asked intelligence agency heads to consider whether they could eliminate the CONFIDENTIAL classification from their classification guides. He suggested this could promote transparency by simplifying classification and focusing personnel on only marking items that would cause significant and demonstrable harm to national security if improperly released. It would also reflect the fact that "few, if any" personnel security clearances or facility or network accreditations were issued at CONFIDENTIAL level and align US markings to those of the UK, "whose classification system successfully eliminated CONFIDENTIAL without impact." Mr Clapper noted that eliminating CONFIDENTIAL would involve a "hard look" at whether material and systems with the marking should be lowered to UNCLASSIFIED or raised to SECRET.[121]

153. In July 2017 the current Director of National Intelligence reported to the ISOO that most agencies had agreed they could eliminate CONFIDENTIAL with "little to no impact on mission." The ODNI, National Geospatial-Intelligence Agency, and National Reconnaissance Office had already removed it from their main guides and would remove it from programme-level guides as they were revised. The CIA would eliminate it in future revisions of its guides. The Defense Intelligence Agency and the NSA had said they needed time to research the impact on their contractors and "long-standing information sharing activities."[122]

Authority to classify

United States

154. Controls on who may apply security classifications, and to what level, have been a regular feature of the US system. Limiting the number of 'original classifiers' has been regarded as a way to reduce or at least limit over-classification, by ensuring that classification authority is limited to people with sufficient experience to apply classifications accurately.

155. Whether it does so is hard to determine. The reported number of original classification authorities within US executive agencies fell from more than 4000 in 2008 to about 2500 in 2009 and has since remained in the low 2000s. The number of original classification decisions has also been reduced dramatically, from more than 200,000 in 2010 to just under 40,000 in 2016, while the estimated number of derivative classification decisions fell from 95 million in 2012 to 55 million in 2016.[123] Reducing the number of original classifiers does superficially

---

119 ISOO Annual Report 2016 at 34.

120 Steven Aftergood "A Bumpy Road for Controlled Unclassified Information" (30 October 2017) Secrecy News <www.fas.org>.

121 James Clapper, "Memorandum: Addendum to the FY 2017 Fundamental Classification Guidance Review" (Office of the Director of National Intelligence, 17 March 2016) available at <www.fas.org>.

122 Mark Bradley, "Memorandum: Director of National Intelligence Supplemental Study to the Fiscal Year 2017 Fundamental Classification Guidance Review" (Office of the Director of National Intelligence, 28 July 2017) available at <www.fas.org>.

123 ISOO Annual Report 2016 at 2.

correlate, therefore, with a reduction in classification decisions. The number of decisions remains colossal, however, and the statistics tell us nothing about their quality. In late 2016 the US Congress heard expert testimony that over-classification remains endemic among government agencies.[124]

Australia

156. Australia does not limit authority for original classification. In 2003-04 the Australian Law Reform Commission considered then abandoned a proposal to do so, on advice from Australian security agencies. [125]

157. The Commission proposed in a discussion paper (on the handling and protection of classified and security sensitive information in legal proceedings) that authority to classify should be limited to experienced officials with seniority and an appropriate security clearance. The Australian Protective Security Manual 2000, in force at the time, did not limit the authority to classify to any particular level of seniority or security clearance.

158. Although the Commission's proposal received some support from submitters, security officials submitted that as agencies created thousands of documents each day it would be "very inefficient" to mandate that only senior and experienced officers could classify information.[126] The Commission accepted this and abandoned its proposal, preferring instead to recommend that protective security policy expressly require minimal classification, provide more guidance on classification, and require staff to be trained in how to classify.[127]

Self-inspection

USA

159. Executive Orders on classification have since 1995 required agencies to conduct self-inspection programmes, including periodic review and assessment of their classification decisions. Since 2010 they have been required to report to the ISOO on these assessments. Their reporting includes data on classification training, delegations of authority to classify and compliance with marking requirements.

160. The ISOO reported last year that all agencies had self-inspection programmes, a small number being "marginal" but some very strong. This was an improvement on ten to fifteen years ago, when a third of agencies did no self-inspection and another third had very weak self-inspection programmes. The Office was concerned however that where agencies identified shortcomings in their own compliance with classification guidance, many did not report any action to correct them.[128]

---

[124] Committee on Oversight and Government Reform, US House of Representatives "Examining the Costs of Overclassification on Transparency and Security: Hearing, 7 December 2016" (US Government Publishing Office, Washington, 2017) Serial No. 114-174.

[125] Australian Law Reform Commission Keeping Secrets: The Protection of Classified and Security Sensitive Information (May 2004).

[126] At [4.35] and [4.38].

[127] At [4.47].

[128] ISOO Annual Report 2016 at 13-18.

161. Shortcomings in self-inspection programmes have also been noted by agency inspectors-general undertaking reviews under the Reducing Over-Classification Act (see below).

162. The Executive Order on classification issued in 2009 by President Obama additionally required agencies to review periodically all their classification guidance, to ensure it was current. Two review cycles have resulted in cancellation of a large number of agency classification guides. In the second review the Navy, for example, reduced its guides from 936 to 421, while the Army cut 77 out of 486 guides.[129] The number remaining is perhaps more striking than the number removed. In any case one expert observer characterises the review as a "housekeeping measure," noting that most of the cancelled guides were eliminated simply because they related to obsolete programmes or technologies.[130]

Declassification

163. Declassification processes have consistently featured in the presidential Executive Orders that set US security classification policy. New bodies have also been established by both the Executive and Congress to expedite declassification.

164. Processes for mandatory review of classification, in response to public requests, and for appeal of decisions arising from review were introduced in the 1970s. These processes still operate. Since 1995 a multi-agency body, the Interagency Security Classification Appeals Panel (ISCAP), has decided appeals on mandatory review. It also rules on appeals from holders of classified information who have filed classification challenges and on agency requests for exemptions from automatic declassification.

165. A requirement for systematic review of 30-year-old classified records was also introduced in the early 1970s.[131] The review requirement fell on the National Archives, however, not the originating agencies, and by the mid-1990s the Archives held 700 million pages of un-reviewed classified records. In 1995 President Clinton issued an Order requiring existing records aged 25 years or more to be automatically declassified unless the originating agency objected. [132] Newly classified material would be declassified automatically after 10 years, with an extension to 25 years possible for certain kinds of information.[133]

166. It was assumed that the requirements for automatic declassification would result in agencies allowing significant amounts of information to be declassified in bulk. Instead they hired more staff and contractors to review records. By 2006 about 1 billion pages had been declassified.[134] The process continues and in 2009 President Obama established a National Declassification Center to review a continuing backlog of records then estimated at more than 400 million pages.

167. The Public Interest Declassification Board considers the 1990s automatic declassification processes outmoded for electronic records. It advocates government investment in automated

---

[129] ISOO Fundamental Classification Guidance Review 2017 <www.archives.gov/isoo/fcgr>.
[130] Steven Aftergood "Secrecy Review Cancels Some Obsolete Secrets" (24 August 2017) Secrecy News <www.fas.org>.
[131] Executive Order 11652, 8 March 1972.
[132] Executive Order 12958, 17 April 1995.
[133] The default period for declassification was extended from 10 years to 25 by President George W Bush in 2003, but returned to 10 years under President Obama in 2009.
[134] Public Interest Declassification Board "Improving Declassification" (December 2007) at 5.

processes for declassification, noting that existing investment is "minimal, at best."[135] The Board has also recommended a shift from declassification triggered by the age of records to topic-based declassification, giving priority to the records that are most important to the public and of most interest to researchers.[136]

168. Despite extensive policy and institutional arrangements for declassification, a scholar at the Brennan Center for Justice has described declassification as "anything but automatic" in the US system. Constraints including lengthy multi-agency 'equity' reviews meant that under current settings "declassification has no chance of keeping pace with classification."[137] Another expert told a Congressional hearing in late 2016 that the National Declassification Center "cranks out the low-hanging fruit from the classified trees, but it has little power over the agencies and continues to pursue a hugely wasteful approach where one classified word can keep a document denied from release."[138]

169. The ODNI reported in December 2016 that the automatic declassification process, which "dwarfs other declassification efforts" in the volume of material released, resulted in release of a substantial amount of material "of minimal interest to historians and researchers, and more broadly, members of the general public." Improving the results would require consistent guidance for all intelligence agencies, to overcome wide variability in approach, and increased funding for "meagrely resourced" declassification programmes. Tools for automating declassification of electronic records would also be essential, but were "years away".[139]

Oversight

170. Within the systems on which I have been able to obtain information, only the US has introduced oversight arrangements and procedures specifically focused on classification activity. Australia and the UK, like New Zealand, make agencies responsible for ensuring their own compliance with classification policy through self-inspection and internal audit. Investigating compliance would be within the remit of the oversight bodies in those countries but has not so far been a priority.

171. The principal US developments in oversight of classification have already been mentioned: the establishment by Executive Order in 1982 of the Information Security Oversight Office (ISOO) and in 1995 of the Interagency Security Classification Appeals Panel (ISCAP).

---

135 Public Interest Declassification Board "The Importance of Technology in Classification and Declassification" (June 2016).

136 Public Interest Declassification Board "Setting Priorities: An Essential Step in Transforming Declassification" (December 2014).

137 Elizabeth Goitein "Eight Steps to Reduce Overclassification and Rescue Declassification: A White Paper Submission to the PIDB" (5 December 2016) <transforming-classification.blogs.archives.gov>.

138 Testimony of Thomas Blanton, Director National Security Archive, George Washington University, to the Committee on Oversight and Government Reform, U.S. House of Representatives, Hearing: Examining the Costs of Over-Classification on Transparency and Security (7 December 2016).

139 Office of the Director of National Intelligence "Improving the Intelligence Community's Declassification Process and the Community's Support to the National Declassification Center" (December 2016).

172. The creation of the Public Interest Declassification Board by an Act of Congress in 2000 can be seen as a further oversight measure.[140] Although purely advisory, the Board has produced substantial and critical public reports on classification policy and procedure.

173. Congress acted again in 2010, passing the Reducing Over-classification Act (ROCA). The Act's measures to reduce over-classification include requiring inspectors-general of national security agencies to assess their compliance with classification policies. The methodology adopted by inspectors-general collectively includes a mixture of desktop policy review, interviews, and sampling of classified documents to assess them for over-classification.[141]

174. A review by the Intelligence Community Inspector-General of ROCA reports on five major intelligence agencies and the ODNI identified common shortcomings in training (particularly on how to make derivative classification decisions) and in self-inspection programmes to monitor the quality of classification decisions.[142] An Inspector-General's evaluation of the Department of Defense found that relevant policies and procedures had been adopted but not always followed or effectively administered.[143] A follow-up three years later found that most of the Inspector-General's recommendations had not yet been fully implemented.[144]

[140] The Board did not actually meet until 2006 as Congress did not appropriate funds for it until late 2005.

[141] Inspector-General, United States Department of Defense "A Standard User's Guide for Inspectors General Conducting Evaluations Under Public Law 111-258, the 'Reducing Over-Classification Act" (22 January 2013, on behalf of the Council of the Inspectors General on Integrity and Efficiency).

[142] Inspector General of the Intelligence Community "Evaluation of the Officer the Director of National Intelligence Under the Reducing Over-Classification Act" (30 December 2014).The five agencies were the Central Intelligence Agency, Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Security Agency, and National Reconaissance Office.

[143] Inspector General of the Department of Defense "DoD Evaluation of Over-Classification of National Security Information" (30 September 2013).

[144] Inspector General of the Department of Defense "Follow up to DoD Evaluation of Over-Classification of National Security Information" (1 December 2016).

3: RE-THINKING CLASSIFICATION

Reforming the system

175. The New Zealand classification system is not dysfunctional, but there is no doubt scope to improve it. Some common observations from users of the system are:

- It asks classifiers to make inherently difficult judgements about degrees of harm to national interests – eg between what will amount to significant damage (requiring a CONFIDENTIAL classification) and what will constitute serious damage (requiring a SECRET classification).
- The distinction between policy/privacy classifications and national security classifications is not widely understood, particularly among officials working outside national security agencies. 'Classified' information is commonly understood as referring only to material classified RESTRICTED and above.
- IN CONFIDENCE and CONFIDENTIAL are very often confused. Many officials naturally assume they mean the same thing and label material CONFIDENTIAL when they mean IN CONFIDENCE.[145] Because 'in confidence' has an everyday (and legal) meaning, officials applying the label to information also commonly do not consider they are classifying it.

176. In addition, my research for this review has indicated that the theory and practice of classification are not entirely aligned in some respects:

- Classification guidance is largely couched in terms consistent with the idea that the content of information determines its risk level and therefore its classification. In fact the higher levels of classification are predominantly applied where the concern is to protect not content but sources.
- The supposedly central distinction between policy/privacy and national security classifications does not align with the central distinction in the level of protection applied to material in modern information systems (see 'The main divide' below).
- Some policy constraints on classification activity appear to be widely ignored, including policy that agencies should limit the duration of protective marking and review the protective marking of information regularly.

177. I have also noted that:

- Agency classification guides do not necessarily provide any more direction than the primary policy material on how to classify.
- There is no systematic effort to collect, compile and report basic statistics on classification activity and classified information holdings.

---

[145] This confusion was noted also in the Australian system pre-2011 – see Australian National Audit Office "Operation of the Classification System for Protecting Sensitive Information" (11 August 1999) at [2.85].

- Systematic declassification generally receives very limited attention and resources.

Categories of official information

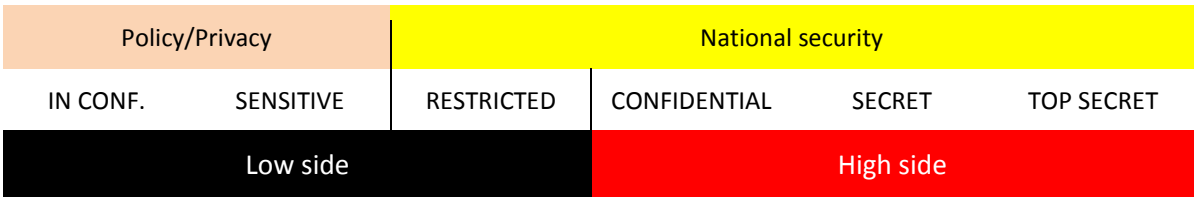
178. With the above issues in mind and taking lessons from other countries' reforms, I have reconsidered the structure of the classification system.

179. Classification is essentially a system of categories. My approach presumes that simplicity is a virtue: good decisions on classification will be made more easily and often if the system is no more complex than necessary. The classification system should therefore have no more categories than necessary.

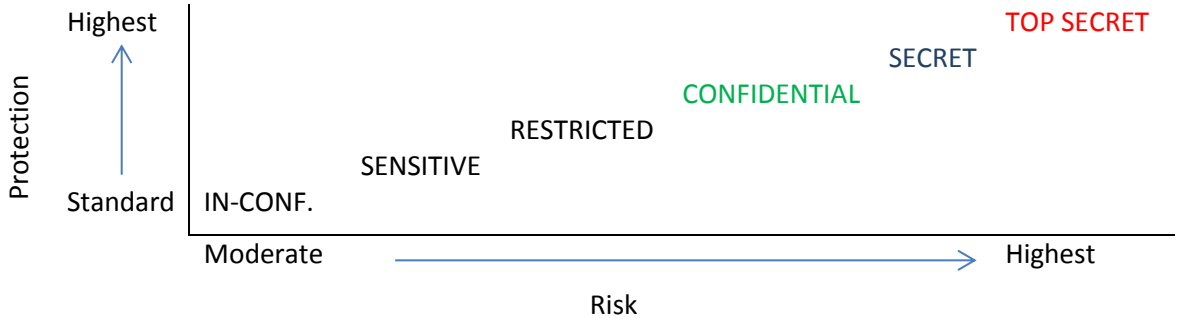
180. I have no argument with the classification system's most basic division of official information into that which requires increased security and that which does not. But what is the next essential division of that category of information requiring increased security?

The main divide

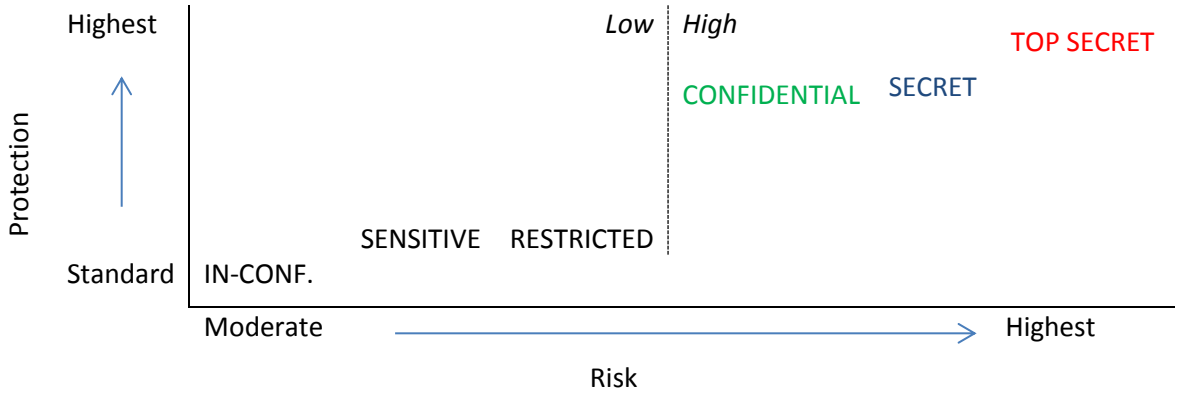
181. There is a disjunction at the heart of the New Zealand classification system. In principle the central division is between national security classifications and policy/privacy classifications. In practice, however, the critical division is between information that must be stored on a high side system (not connected to the internet) and that which can be stored on low side (internet-facing) systems:



182. In principle, classifications rise in a steady progression of risk or sensitivity and the protection given to classified information rises steadily with it:



183. In practice, however, there is little difference in the level of protection between some classifications and a major leap in the middle (from low side to high side):



184. The most consequential result of classification is whether information lands on the high side or the low: whether it has the high protection and constraints on access that follow from being held in isolated systems, or whether it has the lesser protection and freer access that comes from being held in widely-connected systems protected by more standard security measures. The central question for classification is therefore not whether information is 'national security' information or not (from which nothing necessarily follows) but whether it belongs on the high side or the low side.

185. How does a classifier decide whether information belongs on the high or the low? I think the UK classification system provides a good answer. Information belongs on the high side when accidental or deliberate compromise would have serious adverse effects (which can be more fully specified) *and* where it requires protection against highly capable threat actors, such as some state sponsored actors and some highly capable organised crime groups. Information belongs on the low side when it requires more than routine protection, but the potential threats to its security come from attackers with bounded capability and resources, such as 'hacktivists', single-issue pressure groups, competent individual hackers and the majority of criminal individuals and groups.[146]

186. On this basis the reformation of a classification system begins with the distinction between high and low, distinguished on the basis of both sensitivity and threat:

Low side	High side
Information that requires more than routine protection, against threat actors with bounded capability and resources.	Information that requires high protection against highly capable threat actors.

187. I think it important that classification guidance explains clearly that the step from low side to high side is a big one that requires clear justification. The UK guidance effectively describes the equivalent step in their system, from OFFICIAL to SECRET, as a "cliff face".

[146] See Cabinet Office (UK), above n 94 at 7-8.

188. Orienting the classification system around the low/high divide does not mean the concept of national security information becomes meaningless. Most information on the high side of classification will still relate to national security (and some national security related information will, as now, be on the low side). The national security/non-national security distinction only ceases to be an organising principle for classification.

Classification on the high side

189. If there is a clear category of official information that needs to be held and shared on high side systems, is there any need to further divide that category? Is there any need, in other words, for more than one high side classification?

190. It is notable that no classification reform I have looked at has involved the abolition of a SECRET/TOP SECRET distinction. Even the boldest simplification proposals, such as those of the US Joint Security Commission and Public Interest Declassification Board, have accepted that, among secrets, some are particularly sensitive and belong in a category of their own. There is a cogent reason for this: some information, if disclosed, can put a human or technological source (or advantage) at risk; other information (or the same information, sanitised) can provide a valuable information advantage. Both kinds can require careful protection, but the first requires more.

191. The continued recognition of a SECRET/TOP SECRET distinction in the classification systems of New Zealand's intelligence and defence partner countries also makes a single high-side classification impracticable. Partners will not share with New Zealand information they have classified TOP SECRET unless New Zealand will give it equivalent protection. If there was a single high side classification it would have to be TOP SECRET to enable us to continue to receive such information. That would clearly be excessive for a considerable amount of information that otherwise merits high side protection.

192. I think it inevitable, therefore, that the classification system must continue to subdivide high side information into at least the two categories of SECRET and TOP SECRET:

Low side	High side	
	SECRET	TOP SECRET

193. I do not see any compelling reason, however, for any further subdivision of information on the high side.

194. In effect the current system can be understood as further subdividing SECRET information into higher and lower categories labelled SECRET and CONFIDENTIAL. The value of doing this has often been questioned, however, and is not clear to me. Information in the two classifications is subject to near-identical storage and handling requirements. Classification guidance asks classifiers to choose between them on the basis of opaque distinctions between 'damage' and 'serious damage'. The UK has abandoned the distinction and the US intelligence community is apparently in the process of doing so.

195. Eliminating CONFIDENTIAL would simplify classification on the high side, enabling it to be decided by more clearly defined binary choices: first, does the information belong on the high side? Second, should it be SECRET or TOP SECRET? A simpler decision process should enable decisions to be made with more confidence and accuracy.

196. The practical consequences for agencies of eliminating CONFIDENTIAL as a classification would have to be carefully assessed before such a change was made. This would require a consultation exercise beyond the scope of this review.

197. One question would be whether any need currently met by classifying material or technology as CONFIDENTIAL could be met by the use of access controls.

198. A matter of importance would be the impact on security clearance vetting requirements. In recent years there have been about 2500 applications a year for CONFIDENTIAL clearances. Each takes about an hour to process. If all such clearances had to be upgraded to SECRET the time required would double.

199. While eliminating CONFIDENTIAL would no doubt result in the upgrading of some information and equipment and technology to SECRET, it should also result in some being downgraded. (This expectation has been clearly expressed as a transition expectation in both the UK and the US). This downgrading could remove some clearance requirements. It also seems possible that negative vets could still be carried out where required for particular roles. In effect this might mean simply disassociating the current lowest security vetting level from the classification system. A military role that involves operating a particular item of defence technology might require a 'level 1' clearance, for example, that confers no broader presumption of access to classified information.

Classification on the low side

200. We can ask the same question about classification on the low side as on the high: is there any need to divide the category of information that belongs on the low side into sub-categories? Is there any need for more than one low side classification?

201. Again I think there is at least one necessary and meaningful division. It is between information that can be held and managed on systems with standard levels of security – the vast bulk of official information – and information that, even if only temporarily, requires additional protection. Such information might relate to defence, diplomacy (including trade relations), economic and financial policy that could be gamed or undermined if prematurely disclosed, and some aspects of law enforcement, particularly where a person's safety is concerned.

202. In the current classification system this is the distinction between IN CONFIDENCE on the less-protected side and SENSITIVE and RESTRICTED on the more protected side. The key difference in handling is that SENSITIVE and RESTRICTED material must be encrypted for transmission

across public networks, while IN CONFIDENCE material need not be.[147] This is met by use of SEEMAIL in the public sector.

203. On this reasoning there are at least two categories of information on the low side, as there are on the high:

Low side		High side	
Standard security (currently up to IN CONFIDENCE)	Enhanced security (currently SENSITIVE and RESTRICTED)	SECRET	TOP SECRET

204. I question, however, whether IN CONFIDENCE is, or needs to be, a security classification at all.

205. I think that labelling material as "in confidence" (or "confidential", which in plain English means the same thing) is unquestionably useful. The concept of confidentiality is widely understood. It is widely employed in settings familiar to most people, including healthcare, business, finance and other contexts involving the exchange of personal and sensitive information. It has an established meaning at common law. Identifying information as 'in confidence' is, for most people, the obvious first step to protect it beyond the normal level of openness.

206. Labelling material as "in confidence" does not need to be an act of classification to achieve its purpose. Many officials using the label know what they mean – as do the people they exchange it with – but do not consider themselves to be classifying the information. They might have been trained poorly or not at all in use of the classification system. But this does not matter: the use of 'In confidence' generally works anyway.

207. Nor do the storage and handling requirements for IN CONFIDENCE material differ in any substantial way from those for ordinary unclassified official information. Essentially the protection given to IN CONFIDENCE information amounts to marking it and trusting officials and other recipients to handle it with discretion. In my experience this generally occurs.

208. For these reasons I think "In Confidence" should remain available as a label for official information, but not as a classification. It should be, in effect, a caveat that may be used without a classification. This I think will allow "In Confidence" to continue to be used according to its natural and common law meaning. It will also help define more sharply where classification begins, with the application of markings that require a shift from ordinary storage and handling practices to more demanding and restrictive ones:

[147] Manual transmission requirements differ primarily in that SENSITIVE and RESTRICTED material being transmitted between overseas posts should go by diplomatic airfreight, while IN CONFIDENCE material can go by ordinary post or courier. Electronic storage requirements are similar for all three classifications, but give agencies discretion to apply higher levels of security and access control to the higher two. Hard copy storage requirements differ in that SENSITIVE and RESTRICTED material must be kept in a lockable area of cabinet while IN CONFIDENCE requires only the protection of normal government building security. A national security clearance is not required for access to information up to and including RESTRICTED.

Unclassified	Classified		
	Low side	High side	
Standard security (up to "In Confidence")	Enhanced security (currently SENSITIVE and RESTRICTED)	SECRET	TOP SECRET

209. The final question is whether the remaining category of low side information needs to be divided further. The current system divides it into SENSITIVE (for material requiring protection on policy and privacy grounds) and RESTRICTED (for national security information). As with the distinction between CONFIDENTIAL and SECRET, I do not see a need for this.

210. The storage and handling requirements for SENSITIVE and RESTRICTED are essentially the same. The designers of the current system apparently did not see enough difference in the protection requirements for each classification to justify any significant difference in the security applied. Nor do I.

211. Nor does the distinction between national security and non-national security information clearly hold up when the criteria for each existing classification are compared. Serious damage to the economy from premature disclosure of economic or financial policies is arguably a threat to national security on the "all hazards" approach New Zealand has adopted.[148] But the risk of such damage is cause for the policy/privacy classification SENSITIVE under the current system rather than the national security classification RESTRICTED.

212. Essentially I think the current criteria for the SENSITIVE and RESTRICTED classifications correctly identify types of information likely to require the enhanced protection codified by a security classification. But I think those types of information can comprise a single category with a single protection standard. The current system treats them, unnecessarily in my view, as distinct categories subject to a single protection standard.

213. On this basis only one low side classification is required. It could be labelled either RESTRICTED or SENSITIVE. I think however that a new label would probably be a useful signal of change. "Protected" is used in partner countries' systems, generally for mid- to low-level classifications. That is enough for me to suggest it here, but another label could do as well.

214. The step from unclassified (including unclassified "In Confidence") to PROTECTED would be justified if the relevant sensitivity criteria were met (eg endangering the safety of any person, or hindering the security of New Zealand forces) *and* the information required protection from likely active efforts to obtain it, or loss of control through error. This would often apply, for example, to military information of relatively low sensitivity (such as would currently be RESTRICTED). Much information relating to the commercial dealings of government agencies would not however be a *likely* target of external attack, or raise significant risk if, for example,

[148] See Department of the Prime Minister and Cabinet *National Security System Handbook* (August 2016) at 2-3 [IN-C].

it was mistakenly transmitted to the wrong recipient. Such information could be adequately protected by labelling it "In Confidence", as commonly done now.

215. My proposed revised classification system therefore has three levels:

<table>
<tr><td>Unclassified</td><td colspan="3">Classified</td></tr>
<tr><td rowspan="2">May be marked "In Confidence"</td><td>Low side</td><td colspan="2">High side</td></tr>
<tr><td>PROTECTED</td><td>SECRET</td><td>TOP SECRET</td></tr>
</table>

216. I would make one modification to the current criteria for low-side classification. Under the current system information whose improper access or disclosure would prejudice the maintenance of law, including the prevention, investigation and detection of offences and the right to a fair trial, can be classified IN CONFIDENCE but no higher. I think at least some such information will merit the kind of protection provided by a higher classification, such as the protection of encrypted transmission.

217. I have been unable to identify why the current system limits the classification of such information to IN CONFIDENCE. The criteria for a SENSITIVE classification mirror almost exactly the conclusive reasons for withholding information under section 6 of the OIA. The single exception is information whose compromise would prejudice maintenance of the law. The risk of undermining law enforcement and the administration of justice can therefore be a conclusive reason for withholding information under the OIA, but is not a reason for applying more than ordinary protection to such information. I do not see the sense of that. It is not explained in the December 2000 Cabinet paper that proposed the policy and privacy classifications and their criteria and I have been unable to locate the underlying policy advice.

218. It is likely that if some information relating to the maintenance of law needs the protection of a low side classification, it needs it for only a limited time. That can be accommodated, however, by providing for the classification to expire after a specified time or event (eg the conclusion of proceedings).

Unclassified

219. The current policy is that unclassified material may be marked as such, but need not be. I think that is a practical approach and see no reason to change it.

220. An alternative would be to provide for labelling unclassified official information as "official" – either with that word, as in the UK, or with an equivalent such as FOR OFFICIAL USE ONLY. This could be seen as a useful reminder that information held by government is subject to a standard level of security and must be handled responsibly.

221. Under the OIA, however, all information held by government is official information. I do not think that labelling only some of it as "official" would be helpful in that context. There is an implication of ownership in a label like "official" that I think should be avoided when government is the steward rather than owner of much of the information it holds.

222. I suggest too that labelling official information as such should not be necessary to ensure its proper handling by officials in the course of ordinary government business. It should be – and I think is – reasonable to presume that officials are competent to manage routine official information appropriately and need classification only to alert them where special care is required. Ensuring officials understand and meet their basic obligations is a matter of selecting the right employees and ensuring they are properly trained and managed. Labelling can add little to that. I am not aware of any evidence that public servants generally have difficulty discerning or meeting their basic responsibilities concerning official information.

223. Avoiding any routine labelling of ordinary official information helps, in my view, to establish a boundary between what is classified and what is not. UNCLASSIFIED can be treated as a de facto classification, particularly within high side information systems that automatically require protective marking. By far the more widespread understanding, however, is that classified information is a small and distinct subset of official information that has been identified as requiring protection out of the ordinary. I think that is as it should be.

Summary: A simpler system

224. In summary I am suggesting a simplification of the classification system from six to three classifications. The central distinction would be between information that may be stored and transmitted on internet-facing (low side) systems and information that must be stored and transmitted on air-gapped (high side) systems. There would be one low side classification, which could be labelled PROTECTED, and two high side classifications, SECRET and TOP SECRET. Unclassified information could, but need not, be labelled as such. It could also be labelled as "In Confidence", which would not be a classification but a caveat carrying its ordinary legal meaning.

225. My proposed change is from this:

<table>
<tr><td rowspan="3">Unclassified</td><td colspan="2">Policy/Privacy</td><td colspan="4">National security</td></tr>
<tr><td>IN CONF.</td><td>SENSITIVE</td><td>RESTRICTED</td><td>CONFIDENTIAL</td><td>SECRET</td><td>TOP SECRET</td></tr>
<tr><td colspan="3">Low side</td><td colspan="3">High side</td></tr>
</table>

to this:

<table>
<tr><td>Unclassified</td><td colspan="3">Classified</td></tr>
<tr><td rowspan="2">May be marked "In Confidence"</td><td>Low side</td><td colspan="2">High side</td></tr>
<tr><td>PROTECTED</td><td>SECRET</td><td>TOP SECRET</td></tr>
</table>

226. Classification guidance would emphasise that the step up from PROTECTED to SECRET is a large one, justified only when the information is both highly sensitive *and* requires protection from highly capable threat actors.

227. The criteria for SECRET and TOP SECRET would be substantially the same as under the current system, although I think that guidance material could be reviewed to provide more clarity on the distinction between them. Essentially this is that, while both classifications protect information that gives decision-makers a tactical or strategic advantage on matters of national importance (usually national security), TOP SECRET is generally reserved for the protection of information whose disclosure would put information sources or capabilities – human or technical – at risk.

228. The criteria for PROTECTED would effectively be a combination of the current criteria for SENSITIVE and RESTRICTED. In addition, information whose improper access or disclosure would prejudice the maintenance of law, including the prevention, investigation and detection of offences and the right to a fair trial, could be classified as PROTECTED.

229. The step from unclassified (including unclassified "In Confidence") to PROTECTED would be justified if the relevant sensitivity criteria were met (eg endangering the safety of any person, or hindering the security of New Zealand forces) *and* the information required protection from likely active efforts to obtain it, or loss of control through error.

230. 'National security information' could (as now) be classified either on the high side (SECRET or TOP SECRET) or the low side (PROTECTED).

231. I would expect the principal benefit of such a system to be easier, more consistent and more accurate decision-making on classification. This in turn should mean less over- and under-classification and more transparent decisions – ie decisions whose basis is more readily discerned and therefore more amenable to review when required.

232. I make this proposal fully aware that its practicability would need to be carefully tested by consultation with the broad range of government agencies that use the classification system.

233. The implications for interoperability with defence and intelligence partner country systems would need to be assessed in consultation with the relevant authorities in those countries. I have however attempted indicative tables of how the classifications I propose might compare to those of New Zealand's intelligence partners. See Appendix 2.

System ownership

234. The terms of reference for this review include the identification of the appropriate ownership of the classification system.

235. The ultimate owner of the classification system is clearly the Government. The system is administrative policy, applied by Cabinet directive. That is not at issue: 'ownership' here means primary responsibility for implementation and maintenance of the system, including leading advice to the Government on any changes.

236. The policy programme that led to the establishment of the PSR expressly addressed the ownership of the PSR as a whole. It identified the Chief Executive of the Department of the Prime Minister and Cabinet (DPMC) as the owner of the PSR; the Security and Intelligence

Board[149] as its steward, responsible for providing leadership and vision; and the Interdepartmental Committee on Security as its custodian, accountable to the steward for maintenance of the PSR's content and support structures. Specific management responsibilities were also identified: the policy and governance lead was shared by NZSIS and GCSB. The lead agency on information security was GCSB. Management responsibilities were defined as day-to-day management, development and delivery.

237. This scheme suggests leadership of change to the classification system would belong with the Security and Intelligence Board.

238. Leadership of policy development should sit, in my view, with a central agency. The intelligence and security agencies clearly have key roles in any reform of classification, as the government's advisers on personnel and information security and as intensive users of the system. I think it important, however, that any policy change be led by an agency positioned to take a broad view of the needs of the full range of agencies that use the classification system, most of which are not intensive users. The natural focus of the intelligence agencies is on the security and protection of information. I think classification reform should be led by an agency that is familiar with the requirements of national security, but is also outward-facing with a regard for the public interest in open government and the availability of official information. The obvious agency in my view is DPMC. This would be consistent with the nominal ownership of the PSR by the DPMC chief executive.

Classification principles

239. In my view the principles of the current classification are generally valid. I have recommended the abandonment of one of them, namely the idea that the distinction between national security and non-national security information is fundamental. I have no issue with the principles regarding risk assessment, aggregation, originator control, minimal classification and avoidance of classification for improper purposes.

240. There are however two statements of principle from US classification policy that I think could usefully be adopted by the New Zealand system. One is that no information may remain classified indefinitely and any indication to the contrary is invalid.[150] The other is that if there is any significant doubt about the appropriate level of classification, it is to be classified at the lower level.[151] Both principles in my view have the potential to help contain over-classification. Such are the incentives for over-classification that I do not see any real risk that their application might produce the opposite.

---

[149] The Security and Intelligence Board (SIB) is a governance board of the Officials' Committee for Domestic and External Security Coordination (ODESC). ODESC is a committee of departmental chief executives, chaired by the chief executive of DPMC, which has oversight of national security policy and coordinates responses to national security risks. The SIB focuses on external threats and intelligence issues. It is chaired by DPMC's deputy chief executive for security and intelligence and includes officials from DPMC, the intelligence and security agencies, the Ministry of Foreign Affairs and Trade, the Ministry of Defence, New Zealand Customs, the New Zealand Defence Force and the New Zealand police, with others as required.

[150] See eg Executive Order 13526 at section 1.5(d).

[151] Executive Order 13526 at section 1.2(c).

Reducing over-classification

241. My primary proposal to reduce over-classification is my proposed simplification of the classification system. Making classification simpler should make it easier to get it right.

242. The unfortunate lesson from the international reforms I have considered is that nobody has yet identified a singularly effective measure to address this inherent vice of security classification systems. What is required, rather, is a combination of measures applying pressure against over-classification at several points in the 'life cycle' of classified information: from the original (or derivative) decision to classify, through review and declassification.

243. Useful guidance is critical to good classification decisions. From the limited selection of agency guides I have seen, there is scope to improve the extent to which agencies provide direction that supplements rather than repeats PSR guidance. Agencies differ in the extent to which they use high and low side classifications. Their guides should reflect this, giving more extensive guidance on the application of the most relevant classifications (or the use of "In confidence"). Agency guides should make generous use of examples relating to the normal business of the agency. If the classification system is reformed it will be necessary to revise the associated guidance material, both at the PSR and agency levels. This should include testing revised material with staff to get feedback on the extent to which it helps them make classification decisions.

244. Classification system guidance encouraging agencies to review protective marking regularly, such as at the end of a project or event, does not seem to be followed with any regularity or vigour, at least within the intelligence agencies. No doubt it is not and never will be the most pressing question for any review of a completed project or operation. These occasions should however provide a relatively easy opportunity for reconsideration of classifications, while the reasons for applying them are still fresh, with a view to declassifying, downgrading or setting an end date. I think the PSR guidance on review should be more firmly expressed. Agencies should require line and project managers to report (eg to the chief information security officer or compliance manager) when they have done such a review of classified information holdings, with a brief account of the outcome. The agency should review each year the extent to which this is being done.

245. Some measures applied elsewhere with the aim of reducing over-classification do not fit the New Zealand context, in my view. These include the American innovations of creating new classification-focused bodies (such as the ISOO, the Interagency Security Classification Appeals Panel and the Public Interest Declassification Board); more stringent limitation of authority to classify; a more formalised process for classification challenges; and "automatic declassification." Nor do I see any need for statutory intervention comparable to the Reducing Over-classification Act.

246. Establishing any new administrative body requires a compelling case that the benefits will justify the expense and resources involved. The US bodies have been established to meet particular needs in the US system, arising to a significant extent from the sheer scale of the US national intelligence and security apparatus. I see no equivalent need in New Zealand, with the possible exception of new arrangements for declassification, discussed below.

247. In my view practical considerations argue against tighter controls on authority to classify. New Zealand government agencies are relatively small. They increasingly emphasise the value of individual initiative and responsibility rather than hierarchies of control. New Zealand officials commonly perform a broader range of functions than those in larger bureaucracies. Information systems in agencies that deal with sensitive material increasingly require classification of any new document or email. I think it unrealistic, in this setting – and particularly for agencies and officials dealing intensively with classified material – to propose any more significant limitation on who may classify. I also think that a simpler classification system that is easier to apply should not require years of experience to apply accurately.

248. The US classification challenge process, with a right of appeal to ISCAP, produces a relatively insignificant number of reported challenges.[152] Observers have suggested this is because officials, if they are even aware of the process, lack any incentive to dedicate the time and effort required and face a contrary pressure from peers and supervisors not to challenge their colleagues' decisions.[153] This seems right. New Zealand classification system guidance states that protective markings thought to be inappropriate should be queried with the originator.[154] I think this should be retained as a general instruction. I doubt however that a more formal process would be any more effective a check on over-classification than it has been in the US. More productive in my view would be the promotion of a workplace culture in which informal consultation on and questioning of classification decisions is normal.

Facilitating declassification

249. My key proposal for facilitating declassification is a shift to topic-based systematic declassification supervised by a multi-agency group.

250. Ad hoc declassification occurs (sometimes) in response to requests for information under the OIA and Privacy Act. A frustrated requester can seek review of an agency response by the Privacy Commissioner or Ombudsman and in some circumstances by my office. I do not propose any change to these processes.

251. The weakness to be addressed is in systematic classification of classified records. Experience in the US (the only open source of empirical data) shows that systematic declassification is at best a meagre remedy for over-classification: it is laborious and can never keep up. It can however be a source of uniquely valuable historical records. It is also in my view an important observance of the principle that a democratic state may keep secrets, but not forever.

252. Systematic declassification programmes in New Zealand agencies are modest, meagre or non-existent. Where the resources for a task are very limited there is a natural tendency for those labouring at it to reach for the 'low hanging fruit' in an effort to show progress. I found some evidence that this occurs, with priority being given to dealing with the records that are easiest to declassify, rather than those of most historical value.

---

[152] In financial year 2016, a total of 954 formal challenges compared to 39,000 original classification decisions and an estimated 55 million derivative classification decisions – ISOO Annual Report 2016.

[153] Elizabeth Goitein and David Shapiro, "Reducing Overclassification Through Accountability" (Brennan Center for Justice at New York University School of Law, 2011) at 48.

[154] NZGSCS at 4.4.

253. Systematic declassification, where it occurs, is driven to a large extent by the age of the records concerned. It is triggered by the age thresholds in the Public Records Act, or its allowable extensions. I think topical priorities, not just age, should organise the review of classified records – as proposed by the Public Interest Declassification Board in the US.[155] I agree with the Board that this would allow limited resources to be focused on the records most important to the public and of greatest interest to researchers. Topics should be identified through agency and public consultation, including with specialist groups such as historians and academics. Archives NZ would be an important source of advice.

254. As well as increasing the value of the product of systematic declassification, a topic-based approach may prove easier to resource and implement. Review of historical records for possible declassification is generally seen as an unexciting, 'backwater' task. An approach that leads reviewers to churn through uninteresting records for the sake of volume rather than quality only reinforces this. Focused review of records relating to particular periods or events of historical significance should be inherently more rewarding work. It could also be organised as a series of projects, staffed with a shifting roster of relevant officials, including possibly on the basis of part-time commitments or secondments.

255. The organisation of any particular topic-based classification review would depend on where the relevant records were held – eg whether they were predominantly within one or two agencies, or spread across several.

256. In any case the second key element of my proposal is supervision by a group of senior officials drawn from more than one relevant agency. In this I am influenced by the results of the multi-agency ISCAP appeal process in the US, which has frequently ruled in favour of requesters appealing against agency refusals to declassify. One experienced observer, describing the panel as a "rousing success," identified its multi-agency composition as the key factor: "[It] turns out that that simply moving the decision about declassification out of the hands of the original agency makes a huge difference, even when the originators still have a say."[156] It is not that the views of originating classifiers and agencies should be disregarded. A competent review panel will have ample regard for security considerations. The issue I think is that with declassification, just as with classification, there is every incentive for an agency or its representative to err on the side of caution and little or no incentive to favour openness. Bringing more detached perspectives to the process, by including officials from other agencies, is a way to balance that inherent bias.

257. I do not think such a group of senior officials need be a permanent standing committee such as ISCAP. If a project-based, topical approach is taken, it could be a steering group with flexible membership.

258. In making this proposal I have considered and rejected alternatives including "automatic declassification" on the US model. In principle this is the forced declassification of classified material after a fixed period, without review. On closer examination however it unsurprisingly allows agencies to seek exceptions, which they often do. Large volumes of material are certainly

---

155 Public Interest Declassification Board, above n 137.

156 Blanton, above n 133 at 5.

declassified under the US rules. Much commentary suggests however that it is mostly of little or no interest – which is why its declassification is not resisted. I prefer the logic of an approach that targets value.

Training

259. Any change to the classification system would have to be accompanied by a training programme. The more substantial the change, the more extensive the training requirement. The UK experience illustrates the hazards of falling short (see paragraphs 141-143 above).

260. The PSR currently directs agencies to provide all employees with security awareness training, including on protective markings and handling requirements.[157] Holders of a security clearance must be given training when issued the clearance and at least every five years as a condition of maintaining the clearance.[158] I think the PSR should more specifically require training in classification (original and derivative), including the avoidance of over-classification and the review of classifications for downgrading or declassification. The requirement for refresher training should not be limited to the holders of security clearances but to all staff who have cause to classify, including on the low side (eg including officials involved with the preparation of Cabinet papers). Agencies should have internal reporting mechanisms in place to track their compliance with training requirements.

Performance measures

261. The US effort to compile empirical measures of classification activity shows both the difficulty and the value of the exercise. It is difficult to identify effective measures of the quality of decisions made on classification. It is difficult even to quantify the number of decisions made, particularly derivative classification decisions. But there is value in having information that at least indicates broad trends in classification activity. Most analyses of classification issues in the US draw on ISOO data to some extent. I think the public availability of data on classification activity also supports public debate on government secrecy. And there is value in measuring compliance with policy standards, as a spur to remedying poor or non-compliance.

262. I propose that a coordinating agency (eg DPMC, or perhaps the GCIO) consult agency information system managers on the feasibility of establishing some basic ongoing measures of classified data stocks and flows. Collecting such data from agencies for aggregation and analysis would provide at least some empirical information relevant to the ongoing management and development of the classification system. The key matter of interest would be trends over time. Useful data could include, if possible, total holdings of security classified information, by volume and/or items (eg files, documents) and holdings in each classification category. I have already proposed that agencies internally measure their classification review activity (see paragraph 244) and their compliance with requirements for training in classification (see paragraph 260). These measures could also be collated towards a set of basic indicators of system function and performance.

---

157 PSR Protective Security Governance Requirements, Security Awareness Training at 2.5.

158 At 2.1.

263. Such a programme could be piloted with a core set of agencies and subsequently expanded. The potential for developing some basic classification cost metrics, such as those presented by the ISOO, could also be investigated.

Oversight

264. I do not propose any significant change to external oversight of agency classification activity.

265. I have suggested a role for multi-agency supervision of systematic declassification projects (see paragraph 256) and increased self-reporting of classified data management statistics (see 'Performance measures'). Review of classification practices within the intelligence agencies is within the powers of my office. Review of the wider range of agencies that classify official information could be within the remit of DPMC or perhaps SSC. Realistically however other priorities are generally likely to prevail.

266. In my view a primary reliance on self-reporting and self-review is a more practicable and efficient discipline on agency classification activity than reliance on limited oversight and central agency resources. I think this is consistent also with the devolution of protective security responsibilities to agencies under the PSR.

4. SUMMARY OF RECOMMENDATIONS

1. Simplify the classification system:

   1.1. Abandon the distinction between national security and policy/privacy classifications as an organising principle.

   1.2. Organise classification around the distinction between high side information systems (highly secure, non-internet facing) and low side systems (standard or enhanced security, internet-facing).

   1.3. Reduce the number of classifications from six to three: two high side classifications (SECRET and TOP SECRET); one low side classification (PROTECTED):

   - Information currently classified CONFIDENTIAL would be either SECRET or PROTECTED;
   - Information currently classified RESTRICTED or SENSITIVE would be classified PROTECTED;
   - Information currently classified IN CONFIDENCE could be marked "In Confidence" but this would not be a classification.

   1.4. Provide classification guidance emphasising that the step up from PROTECTED to SECRET is a large one, justified only when the information is both highly sensitive *and* it requires protection from highly capable threat actors.

   1.5. Provide for the classification as PROTECTED of information whose improper access or disclosure would prejudice the maintenance of law, including the prevention, investigation and detection of offences and the right to a fair trial.

2. Recognise the Department of the Prime Minister and Cabinet as the appropriate owner of the classification system and the appropriate leader of any change.

3. Retain current classification system principles (with the exception of the distinction between national security and policy/privacy classifications). Add the principles that:

   - no information may remain classified indefinitely; and
   - if there is any significant doubt about the appropriate level of classification, it is to be classified at the lower level.

4. Revise agency classification guides, ensuring they supplement not repeat primary classification guidance, using agency-specific examples. Test revised guides with staff.

5. Strengthen guidance to agencies on review of protective marking. Require them to review each year the extent and outcome of review activity.

6. Adopt a topic-based approach to systematic declassification of historic classified records, supervised by a multi-agency group. Consult the public, experts and Archives New Zealand on priorities for review.

7. Develop a training programme to accompany classification reform. Specify the requirements for ongoing training in classification with more particularity. Extend the requirement for refresher training beyond the holders of security clearances. Require agencies to track their compliance with training requirements.

8. Task a coordinating agency with consulting agencies on the feasibility of establishing basic ongoing measures of classified data stocks and flows. Compile this information with agency measures of their classification review activity and their compliance with training requirements. Use this information to start building a set of basic indicators of classification system function and performance.

APPENDIX 1: TERMS OF REFERENCE

PURPOSE

To identify changes that could be made to the New Zealand security classification system to improve security, reduce costs and increase transparency.

SCOPE AND APPROACH

1. The review will:

    1.1. Compile, from existing material, a concise account of the systems and processes, including terminology, definitions and information handling practices, that make up the classification system;

    1.2. Identify the appropriate ownership of the classification system;

    1.3. Seek empirical measures of the performance of the classification system;

    1.4. Review international literature on classification system issues and reform;

    1.5. Identify gaps between NZ and best practice;

    1.6. Develop recommendations for improvement to the operation of the NZ classification system across government, including through initiatives to:

    1.6.1. reduce over-classification; and

    1.6.2. facilitate declassification;

    1.7. Where possible, identify options for measuring and monitoring the effects of initiatives designed to improve the performance of the classification system;

    1.8. Identify any opportunities for structural reform of the classification system through simplification, having regard to existing national polices and the system's international context.

2. In forming recommendations, security, cost and transparency benefits will be given equal priority.

3. Control system markings and dissemination control markings are not under review.

OUTPUT

4. The review will result in a written report with recommendations to the owner of the classification system and the PERSEC Review Steering Committee, classified at the lowest possible level appropriate.

5. The review is intended to inform the PERSEC review but an account of the review may be published in the Annual Report of the Inspector-General of Intelligence and Security, having regard to its classification.

PROCESS

6. The Office of the Inspector-General will conduct the review and draft the report. 6.

7. The New Zealand Security Intelligence Service and the owner of the classification system will be invited to comment on a draft of the review report.

8. The Inspector-General may invite comment from other New Zealand Intelligence Community Agencies on a draft of the review report.

9. The Inspector-General will consider any comments received before issuing a final report. 9.

TIMING

10. The Inspector-General will seek to prepare a draft report by 31 October 2017.

APPENDIX 2: FIVE EYES CLASSIFICATION COMPARISONS

Table 1: Existing New Zealand classifications compared with partner classifications

USA →	**NZ →**	**USA**
TOP SECRET	TOP SECRET	TOP SECRET
SECRET	SECRET	SECRET
CONFIDENTIAL	CONFIDENTIAL	CONFIDENTIAL
UNCLASSIFIED: FOR OFFICIAL USE ONLY (FOUO)	RESTRICTED	CONFIDENTIAL or FOUO
	SENSITIVE	CONFIDENTIAL or FOUO
	IN CONFIDENCE	FOUO
UNCLASSIFIED	UNCLASSIFIED*	UNCLASSIFIED or FOUO
*[U] information from the US is withheld from the public unless the originator approves release – ie is handled as [U] but treated as in confidence for the purposes of the OIA.		

AUSTRALIA →	**NZ →**	**AUSTRALIA**
TOP SECRET	TOP SECRET	TOP SECRET
SECRET	SECRET	SECRET
CONFIDENTIAL	CONFIDENTIAL	CONFIDENTIAL
	RESTRICTED	FOUO
PROTECTED	SENSITIVE	
Sensitive (DLM)		
FOUO		
	IN CONFIDENCE	
Unclassified	UNCLASSIFIED	Unclassified

CANADA →	**NZ →**	**CANADA**
TOP SECRET	TOP SECRET	TOP SECRET
SECRET	SECRET	SECRET
PROTECTED C		
CONFIDENTIAL	CONFIDENTIAL	CONFIDENTIAL
PROTECTED B		
PROTECTED A	RESTRICTED	
	SENSITIVE	PROTECTED A
	IN CONFIDENCE	PROTECTED B
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED

UK →	**NZ →**	**UK**
TOP SECRET	TOP SECRET	TOP SECRET
SECRET	SECRET	SECRET
	CONFIDENTIAL	
OFFICIAL – SENSITIVE	RESTRICTED	OFFICIAL – SENSITIVE
OFFICIAL	variable	
	UNCLASSIFIED	OFFICIAL

Table 2: Proposed New Zealand classifications compared with partner classifications

These are estimated comparisons only. Where alternatives are given, the first is the default, the second might be applied by agreement with the originator.

USA →	**NZ**	**NZ →**	**USA**
TOP SECRET	TOP SECRET	TOP SECRET	TOP SECRET
SECRET	SECRET	SECRET	SECRET
CONFIDENTIAL	SECRET or PROTECTED	PROTECTED	CONFIDENTIAL or FOUO
UNCLASSIFIED (FOUO)	PROTECTED or In Confidence	In Confidence	FOUO
UNCLASSIFIED	In Confidence	Unclassified	UNCLASSIFIED or FOUO

AUSTRALIA →	**NZ**	**NZ →**	**AUSTRALIA**
TOP SECRET	TOP SECRET	TOP SECRET	TOP SECRET
SECRET	SECRET	SECRET	SECRET
CONFIDENTIAL	SECRET or PROTECTED	PROTECTED	PROTECTED or Sensitive
PROTECTED	PROTECTED	In Confidence	FOUO
Sensitive (DLM)		Unclassified	Unclassified
FOUO	PROTECTED or In Confidence		
Unclassified	Unclassified		

CANADA →	**NZ**	**NZ →**	**CANADA**
TOP SECRET	TOP SECRET	TOP SECRET	TOP SECRET
SECRET	SECRET	SECRET	SECRET
PROTECTED C		PROTECTED	CONFIDENTIAL or PROTECTED A
CONFIDENTIAL	SECRET or PROTECTED	In Confidence	PROTECTED A
PROTECTED B		Unclassified	Unclassified
PROTECTED A	PROTECTED or In Confidence		
UNCLASSIFIED	Unclassified		

UK →	**NZ**	**NZ →**	**UK**
TOP SECRET	TOP SECRET	TOP SECRET	TOP SECRET
SECRET	SECRET	SECRET	SECRET
OFFICIAL – SENSITIVE	PROTECTED	PROTECTED	Per Cabinet Office guidance*
OFFICIAL	In Confidence	In Confidence	OFFICIAL
		Unclassified	

* The UK has specific guidance on handling of international information at RESTRICTED level.

APPENDIX 3: CHANGES IN NZ CLASSIFICATION CRITERIA

1951[159]	1982[160]	2000[161]
TOP SECRET Documents or information, the unauthorised disclosure of which would cause exceptionally grave damage to the nation.	TOP SECRET Information or material the unauthorised disclosure of which is likely to damage national interests in an exceptionally grave manner.	TOP SECRET Compromise of information would damage national interests in an exceptionally grave manner.
SECRET Documents or information, the unauthorised disclosure of which would endanger national security, cause serious injury to the interest or prestige of the nation, or any governmental activity thereof, or would be of great advantage to a foreign nation.	SECRET Information or material the unauthorised disclosure of which is likely to damage national interests in a serious manner.	SECRET Compromise of information would damage national interests in a serious manner.
CONFIDENTIAL Documents or information, the unauthorised disclosure of which, while not endangering the national security, would be prejudicial to the interests or prestige of the nation, any governmental activity, or would cause administrative embarrassment, or difficulty, or be of advantage to a foreign power.	CONFIDENTIAL Information or material the unauthorised disclosure of which is likely to damage national interests in a significant manner.	CONFIDENTIAL Compromise of information would damage national interests in a significant manner.
RESTRICTED Documents or information (other than that described above) which for security reasons should not be published or communicated to anyone except for official purposes.		RESTRICTED Compromise of information would be likely to affect the national interest in an adverse manner.
		SENSITIVE Compromise of information would be likely to damage the interests of the New Zealand government or endanger the safety of its citizens.
		IN CONFIDENCE Compromise of information would be likely to prejudice the maintenance of law and order, impede the effective conduct of government in New Zealand or affect adversely the privacy of its citizens.

[159] Committee on Official Information *Towards Open Government (2) Supplementary Report* (July 1981) n 3 at 40.
[160] Cabinet Directive on Security Classification CO (82) 14 (17 December 1982).
[161] Cabinet Minute "Protection of Official Information" CAB (00) M 42/4G(4) (18 December 2000).

APPENDIX 4: TIMELINE OF CHANGES TO THE NZ CLASSIFICATION SYSTEM

Events		*Classification system developments*
	1951	Classifications are: TOP SECRET SECRET CONFIDENTIAL RESTRICTED
Danks Committee recommends narrowing scope for classification. Official Secrets Act is repealed. Official Information Act is passed.	1982	RESTRICTED classification is abolished. Classifications are: TOP SECRET SECRET CONFIDENTIAL
E-government developments and intelligence sharing highlight issues with classification system.	2000	RESTRICTED classification is restored and policy/privacy classifications are introduced. Classifications are: TOP SECRET SECRET CONFIDENTIAL RESTRICTED SENSITIVE IN CONFIDENCE
Commercially sensitive Cabinet material is improperly disclosed.	2006	
	2007	Endorsement 'SPECIAL HANDLING REQUIRED' is introduced, for use with SENSITIVE classified Cabinet papers.
Government protective security arrangements are reviewed.	2013	
	2014	Cabinet adopts *Protective Security Requirements* as primary source for classification policy, replacing *Security in the Government Sector* manual.