

UNCLASSIFIED

UNDER

THE INQUIRIES ACT 2013

IN THE MATTER

A GOVERNMENT INQUIRY INTO OPERATION
BURNHAM AND RELATED MATTERS

**Memorandum on behalf of the Department of the Prime Minister and Cabinet,
Government Communications Security Bureau and New Zealand Security
Intelligence Service in Response to Minute No 3 of Inquiry**

10 August 2018

Solicitor Acting:
Aaron Martin
Crown Law Office

Department contacts:
DPMC:
Annabel Ritchie

GCSB / NZSIS:
Andrew King

UNCLASSIFIED

Introduction

1. The Department of the Prime Minister and Cabinet (**DPMC**), Government Communications Security Bureau (**GCSB**) and New Zealand Security Intelligence Service (**NZSIS**) agree with the preliminary views expressed by the Inquiry in its Minute No 3 of 19 July 2018 (**Minute 3**) at paragraph 25. DPMC, GCSB and NZSIS appreciate the opportunity to comment on the Minute.
2. DPMC, GCSB and NZSIS have also had the opportunity to review the draft submissions for the New Zealand Defence Force (**NZDF**) and the Ministry of Foreign Affairs and Trade (**MFAT**) in response to Minute No 3, and agree with the views expressed in them.
3. DPMC, GCSB and NZSIS do not have core participant status in the Inquiry. However, DPMC, GCSB and NZSIS hold information that may be relevant to the Inquiry and for that reason each agency does have an interest in aspects of the Inquiry.
4. DPMC, GCSB and NZSIS are committed to assisting the Inquiry and aim to provide the Inquiry with any relevant information that they hold or control.
5. The purpose of this submission is to:
 - 5.1 indicate DPMC's interests in the Inquiry, including classified information;
 - 5.2 supplement the submissions of NZDF and MFAT with more details about GCSB and NZSIS information;
 - 5.3 propose a procedure by which any relevant GCSB and NZSIS information is provided to the Inquiry.

DPMC's interest in the protection of classified information

6. The business units of DPMC that may hold relevant information are:
 - 6.1 The Cabinet Office, which provides impartial secretariat services to the Executive Council and Cabinet. It also provides advice on procedural matters contained in the Cabinet Manual. The Cabinet

Office is the holder of Cabinet decisions for the current and former administrations.

- 6.2 The Policy Advisory Group, which provides 'free and frank' (politically impartial) advice to the Prime Minister, and sometimes to other Ministers.
 - 6.3 The National Security Group, which is responsible for providing coordinated advice on national security to the government, including on the Government Security Classification System.
7. DPMC also has an interest in the matters raised in these submissions, and the submissions of the other Crown agencies, due to its role in administering the Government Security Classification System. To assist the Inquiry, a description of this system, including its purpose, is set out in **Appendix A**.

Production and disclosure of information held by GCSB and NZSIS

8. While Crown agencies have a shared view of the law applicable to the Inquiry, DPMC, GCSB and NZSIS consider it would be appropriate for the Inquiry to adopt slightly different procedures in respect of GCSB and NZSIS information.¹ This extends to GCSB and NZSIS information held by other Crown agencies (such as NZDF).
9. Factors that support the Inquiry adopting a different procedure in respect of GCSB and NZSIS information, in comparison to information of other Crown agencies, are:
 - 9.1 the intelligence relationships GCSB and NZSIS have with international intelligence partner agencies (**intelligence partners**) are of a different nature to diplomatic and defence relationships;
 - 9.2 a greater proportion of the information held by GCSB and NZSIS is at higher security classifications and of greater security sensitivity than that held by other Crown agencies; and

¹ Any information of the National Assessments Bureau (NAB) within DPMC may be similar to GCSB and NZSIS information. DPMC has not yet confirmed whether any NAB information is likely to be relevant to the Inquiry.

9.3 at this early stage, it is unclear to what extent, if any, the Inquiry is interested in the activities of GCSB or NZSIS or the information the agencies hold that is not otherwise held by NZDF.

10. In the event the Inquiry wishes to receive GCSB or NZSIS information, the Inquiry will need to consider issues associated with information that intelligence partners retain an element of control over (**partner-controlled information**), and issues of information with high security classification.

Control of information in international intelligence and security relationships

11. International intelligence and security relationships – an element of the international relationships between governments – operate with a degree of independence from, and in slightly different ways to other aspects of government international relationships. One of the differences between intelligence and security relationships and other governmental relationships is the greater emphasis placed on the security of information.
12. GCSB and NZSIS have obligations to handle information obtained from, or through co-operation with, intelligence partners consistently with requirements determined by those partners. These obligations may explicitly attach to particular information (for example, in a written caveat applied to an intelligence report received by GCSB or NZSIS), but are often an implicit condition of co-operation and information exchange within an intelligence relationship (for example, if the information was obtained by GCSB or NZSIS through use of an intelligence partner's source or method).
13. These obligations to handle information consistently with intelligence partner requirements are not agreed in treaties between states, and are not necessarily defined in other documents. They instead arise as a commonly understood element of international intelligence relationships.
14. One of the handling requirements often applicable to information obtained by GCSB or NZSIS is a requirement for the GCSB or NZSIS to disclose the information to other parties only with the permission of the intelligence partner (or partners) that supplied (or otherwise hold an interest in) the information. This allows the intelligence partner to control the dissemination of that information.

15. The scope of the default partner permission for GCSB or NZSIS to disclose partner-controlled information will vary between categories of information. For a significant amount of partner-controlled information (including many intelligence reports), GCSB and NZSIS are permitted to disclose that information to any personnel in other New Zealand Government agencies who hold an appropriate security clearance and have been briefed into any applicable information compartments.² For more sensitive partner-controlled information, an intelligence partner may only grant permission for GCSB or NZSIS to disclose that information to specific, named (ordinarily senior) government officials and ministers.
16. GCSB or NZSIS will seek further partner permission if they wish to disclose information to recipients beyond the scope initially permitted by an intelligence partner.
17. The scope of default permission to disclose partner-controlled information is unlikely to permit GCSB or NZSIS to disclose such information to inquiries established under the Inquiries Act 2013. Accordingly, GCSB and NZSIS are likely to need to seek partner permission to disclose partner-controlled information to the Inquiry in order to act consistently with their obligations to partners.
18. GCSB and NZSIS have not yet sought partner permission to disclose any information to the Inquiry. GCSB and NZSIS currently anticipate that partners are only likely to grant GCSB or NZSIS permission to disclose information to the Inquiry if the partner has clear assurances about how the information will be handled. These assurances may include that the information will not, through the Inquiry process, be provided to persons who do not hold an appropriate security clearance.
19. Intelligence partners may be willing to permit GCSB and NZSIS to disclose some information to the Inquiry with a lower level of assurance in place. For example, a partner may permit GCSB or NZSIS to disclose a redacted

² Information compartments are a mechanism for ensuring that information of certain types is only provided to those persons with a “need to know”. “Sensitive Compartmented Information” (SCI) is a form of compartmented information. Persons with a need to access the information in a compartment will be given a special briefing before they are permitted to access the information. Compartmented information is often subject to additional security requirements. See protectivesecurity.govt.nz for more information.

document (that excludes some sensitive information) or a summary, to the Inquiry without prior assurances about who will receive the information.

20. An intelligence partner (and the government of that agency) would be likely to be extremely dissatisfied with the New Zealand Government if GCSB or NZSIS were to disclose information to a recipient (such as the Inquiry) without that partner's permission. Such disclosure would also be likely to diminish the views that other intelligence partners and governments have of GCSB, NZSIS, and the New Zealand Government. Accordingly, such disclosure would have a prejudicial effect on the international relations of New Zealand.
21. Additionally, such disclosure would be likely to reduce the willingness of the particular intelligence partner and other agencies to co-operate with and disclose information to GCSB and NZSIS in the future. This has potentially severe consequences for the ability of GCSB and NZSIS to perform their functions effectively, given both agencies rely significantly on partner co-operation and information.
22. Finally, GCSB and NZSIS also rely on this "control" mechanism in respect of information GCSB and NZSIS provide to intelligence partners. This mechanism allows GCSB and NZSIS to manage the risk of partners disclosing sensitive New Zealand information, and prevent information being used to conduct acts that may infringe human rights recognised by New Zealand law. Partners are likely to be less inclined to respect GCSB or NZSIS control over information if they believe GCSB or NZSIS are not reciprocating that respect for their information.

Sensitivity and volume of GCSB and NZSIS information

23. GCSB and NZSIS hold the New Zealand Government's most sensitive information. That information may reveal the details of intelligence targets, sources and methods of obtaining intelligence, and security risks to New Zealand and other countries. The sensitivity of that information means it is subject to the highest level of protection. While NZDF and other Crown agencies do hold similar information (for example, information about the operations of the New Zealand Special Air Service is of comparable sensitivity), the protection able to be applied to much of the information held

by other Crown agencies is necessarily limited by the fact that the work of those agencies is publicly known.

24. A high proportion of GCSB and NZSIS information is of a very sensitive nature compared to other Crown agencies. The nature of GCSB and NZSIS as New Zealand's specialist intelligence agencies means that their work and much the information they hold necessarily involves dealing with sensitive matters. This is reflected by the fact that all GCSB and NZSIS personnel are required to hold the highest level of security clearance granted by the New Zealand Government given their routine access to highly classified information.
25. A significant majority of any GCSB or NZSIS information relevant to the Inquiry is likely to be sensitive and subject to a national security classification. In the same way as intelligence partners, GCSB and NZSIS may seek a level of assurance about how information provided to the Inquiry will be handled (whether or not that is partner-controlled information).

Degree of Inquiry interest in GCSB and NZSIS activities and information

26. GCSB and NZSIS both provided intelligence support to NZDF's Afghanistan operations. GCSB and NZSIS have not publicly confirmed whether or not they supported any particular NZDF operations, including the particular operations at issue before the Inquiry.
27. The Inquiry has not yet had the opportunity to assess the degree to which it is concerned, if at all, with GCSB or NZSIS activities or information belonging to the two agencies. The Inquiry may not wish to consider GCSB or NZSIS activities (particularly given the associated inquiry being conducted by the Inspector-General of Intelligence and Security), or may only wish to consider a limited amount of GCSB or NZSIS information.
28. The degree of the Inquiry's interest in GCSB and NZSIS activities and information may affect the procedure the Inquiry wishes to use for accessing information belonging to those agencies.

Proposed procedure for GCSB and NZSIS information

29. In its submission, NZDF proposes a possible approach to providing classified information to the Inquiry and seeks the Inquiry's views on that model, so that the model can be explored with NATO and other partners.

30. In light of the different nature and quality of GCSB and NZSIS information, the process proposed below would involve managing the provision of GCSB and NZSIS documents to the Inquiry on a case-by-case basis – with each document dealt with according to its specific nature.

Classified summary of GCSB and NZSIS support to NZDF

31. GCSB and NZSIS suggest that, to assist the Inquiry in assessing its level of interest in GCSB and NZSIS information, GCSB and NZSIS would initially provide the Inquiry with a summary of intelligence support provided to NZDF that may be relevant to the matters before the Inquiry. This summary would be classified, but would not contain any partner-controlled information meaning GCSB or NZSIS would not need to obtain intelligence partner permission to disclose it to the Inquiry. At the time of submitting this summary to the Inquiry, GCSB and NZSIS would likely apply for a permanent order under section 15 of the Inquiries Act that would prevent other parties and the public from accessing sensitive information in that summary (other than in an unclassified redacted or summarised form).
32. Based on its review of the summary, the Inquiry would notify GCSB and NZSIS of any matters related to GCSB or NZSIS activities that the Inquiry wishes to receive documents on. GCSB and NZSIS would collate documents relevant to any matters identified by the Inquiry.

Procedure for disclosing GCSB and NZSIS documents to the Inquiry

33. Depending on the nature of the identified documents, GCSB and NZSIS would use one of the following options to provide the document to the Inquiry:
- 33.1 GCSB or NZSIS would provide the document to the Inquiry without any further action;
- 33.2 GCSB or NZSIS would provide the document to the Inquiry and apply for a permanent order under section 15 of the Inquiries Act, including assurance that the document will not be disclosed to other participants or the public (other than in an unclassified redacted or summarised form). Among other reasons for applying for such an order, an intelligence partner may be willing to permit GCSB or

NZSIS to provide partner-controlled information to the Inquiry on the basis that GCSB or NZSIS will apply for such a section 15 order at the time of providing it; or

- 33.3 prior to providing the document to the Inquiry, GCSB or NZSIS would apply for a permanent order under section 15 of the Inquiries Act, including assurance that the information will not be disclosed to other participants or the public (other than in an unclassified redacted or summarised form). Among other reasons for applying for such an order at this time, issuing such an order may provide an intelligence partner with sufficient assurance for them to permit GCSB or NZSIS to disclose partner-controlled information to the Inquiry. With a section 15 order in place and sufficient partner permission, GCSB and NZSIS would provide the document to the Inquiry.
34. When applying for an order under section 15 of the Inquiries Act, GCSB and NZSIS will provide reasons why disclosure of the document would pose a present and real risk of prejudice to the security, defence, or international relations interests of New Zealand.
35. GCSB and NZSIS will also provide reasons for pursuing an option under paragraph 33(b) or (c) above. If GCSB or NZSIS pursue the option under paragraph 33(c), GCSB and NZSIS will provide the Inquiry with evidence to support the issue of a section 15 order, which will include a redacted or summarised version of the document at a lower classification where possible.
36. GCSB and NZSIS suggest the procedure in paragraphs 33 to 35 above also be used in respect of any GCSB or NZSIS information held by other Crown agencies.

Procedure for providing information to other participants and disclosure to the public

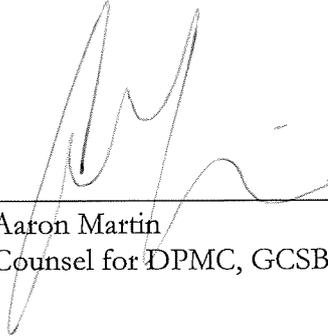
37. In respect of GCSB and NZSIS information provided to the Inquiry using the proposed process above, the Inquiry could then apply the procedure it adopts for providing NZDF and other Crown information to other participants and disclosing such information to the public (such as the approach suggested in paragraph 36 of NZDF's submission).

38. This would be subject to the limit that, under any procedure the Inquiry settles on, any information that is subject to a permanent section 15 order would not be eligible to be disclosed to other participants.

Assistance by an independent person

39. DPMC, GCSB and NZSIS endorse the position expressed in paragraphs 37 and 38 of NZDF's submission regarding assistance by an independent person.

10 August 2018



Aaron Martin
Counsel for DPMC, GCSB and NZSIS

Appendix A – The New Zealand Government Security Classification System

1. The ultimate owner of the Government Security Classification System is the Government. The system is an administrative policy, applied under the authority of Cabinet. The primary source of policy on classification is the Protective Security Requirements (PSR) which were approved by Cabinet. The Government Security Classification System is a policy within the PSR. The Chief Executive of DPMC has a key role in the management of the PSR.

Why is there a Government Security Classification System?

2. The purpose of the Government Security Classification System is to identify official information that requires special protection in order to protect national or individual interests.
3. The system identifies official information that requires extra protection against unauthorised or accidental disclosure and restricts access to that information through a series of controls such as protective markings, handling and transmission requirements and physical and technical barriers (such as separate IT systems which only authorised persons can access, firewalls, encryption, safes and storage facilities).
4. The identification and protective marking of material is based on a risk-assessment of how much damage or prejudice would result if specific content was disclosed. This includes material where disclosure would be detrimental to New Zealand citizens, the New Zealand Government and government agencies.
5. Security clearance rules further define who may have access to information in each classification category. The suitability for access to information is determined through a range of assessment processes that are appropriate to the sensitivity of the information in question, for example, access to national security classified information is dependent on holding a national security clearance, and a valid 'need to know' the information. In addition, certain protectively marked information may bear a compartmented marking in addition to a security classification. A compartmented marking is a word indicating that the information is in a specific need-to-know compartment and is subject to specific briefings, access and handling requirements.

6. The fundamental rule for all aspects of information security is the need-to-know principle. This principle holds that only people who have a legitimate requirement to know the information in order to complete official business should receive the classified information. People are not provided access to classified information because it would be convenient for them to know the information, or by virtue of their status, position, rank or level of authorised access (i.e. security clearance).
7. A security classification specifies how people must protect the information and equipment that they handle. These rules differ depending on the classification attached to the information, with more highly classified information subject to more stringent controls.
8. Classifications are not mandated or required by statute. It is an administrative matter, applied within existing legal frameworks which give the public rights of access to official information, and uphold the public interest values of open government. The classification system does not undermine those legal frameworks, but works within them.
9. There are two broad categories of classification: material that needs to be protected because of national security, and material that needs to be protected because of public interest or personal privacy.
10. National security information is defined in the Government Security Classification System as ‘... any official information or resource, including equipment that records information or is associated with New Zealand’s:
 - 10.1 protection from espionage, sabotage, politically-motivated violence, promotion of communal violence, attacks on New Zealand’s defence system, acts of foreign interference;
 - 10.2 protection of New Zealand’s territorial and border integrity from serious threats;
 - 10.3 defence plans and operations;
 - 10.4 international relations, significant political and economic relations with international organisations and foreign governments;

- 10.5 law enforcement operations where compromise could hamper or make useless national crime prevention strategies or particular investigations or adversely affect personal safety; and
 - 10.6 national interest that relates to economic, scientific or technological matters vital to New Zealand's stability and integrity.
11. The System notes that not all information about these matters needs to be protectively marked. It should only be marked if its compromise, disclosure or misuse could damage national security, the Government, commercial entities or members of the public.
12. Security classifications for material that needs to be protected because of national security are:
- 12.1 Restricted - is used when the disclosure of information would be likely to affect the national interests in an adverse manner.
 - 12.2 Confidential - is used when the disclosure of information would damage national interests in a significant manner.
 - 12.3 Secret - is used when the disclosure of information would damage national interest in a serious manner.
 - 12.4 Top Secret - is used when the disclosure of information would damage national interest in an exceptionally grave manner.
13. Information that requires protection, but not for national security reasons can relate to public interest or personal privacy matters. These protective markings include:
- 13.1 In-Confidence - is 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 adversely affect the privacy of its citizens.
 - 13.2 Sensitive - is used when the compromise of information would be likely to damage the interest of New Zealand or endanger the safety of its citizens.

14. The basis and requirements for each of these classifications is set out below.

What interests are protected under the System?

National security

15. National security is the condition which permits the citizens of a state to go about their daily business confidently free from fear and able to make the most of opportunities to advance their way of life. It encompasses the preparedness, protection and preservation of people, and of property and information, both tangible and intangible.³ There is a strong national and public interest in ensuring that national security information is protected.
16. The unauthorised disclosure of classified information would be likely to cause damage of varying degrees of severity to national security and/or the defence, economic, foreign relations and political interests of the New Zealand Government, endanger the safety of New Zealand citizens, obstruct the maintenance of law and order or impede the effective conduct of government in New Zealand. The information classification system recognises that at the most severe end of this spectrum, unauthorised disclosure of information would be likely to cause exceptionally grave damage to the above interests, and accordingly imposes appropriately stringent information protection and disclosure restrictions.
17. It is important to note that the potential threat to national security goes further than the risks posed by the unauthorised disclosure of information (for example, disclosure of specific details of a document, email or phone call) to third parties. In addition to these security risks, the disclosure of specific information could inadvertently lead to the uncovering of intelligence-gathering sources and methods, for example, the identification of an undercover intelligence agent or an informer whose safety would be compromised, the disclosure of counterintelligence and encryption methods, which would render methods ineffective in the future or intelligence assessments designed to show evidence of fraud.
18. Protecting national security also means safeguarding the confidence our partners have in us as well as protecting the methodologies and sources used, given the potential consequences of those being made public. Failure to

³ Department of the Prime Minister and Cabinet - National Security System Handbook, August 2016

protect information supplied to us by our partners at levels equivalent to those they would apply would risk endangering the continuing provision of such information to us, with consequential harm to our national interests.

Public interest and personal privacy

19. As noted above, the classification system also covers information that needs to be protected because of other public interest concerns (beyond national security). For example, in order for the Prime Minister and Ministers to effectively carry out their role, they must be able to receive and rely on, with confidence, free and frank advice from their advisers. It is in the public interest for them to receive such advice. The advice is often provided under extreme time pressures, and in many situations from confidential sources. Although the advice provides a clear message, there is often no time for the more careful drafting that would be required if the advice was to be disclosed out of context. This kind of information is classified because the disclosure of such information could prejudice the future supply of similar information or information from the same source. The disclosure of information may also undermine the relationship of trust between the Ministers and their advisors so that the future provision of free and frank advice would be inhibited.
20. Similarly, the classification system is also used to protect information entrusted to the government where the disclosure could adversely affect the privacy of New Zealanders, for example, an individual's medical records. The disclosure of such information to third parties would have a prejudicial impact on private individuals and undermine the confidence the public has in the Government Security Classification System.

Approach to disclosure of classified information / declassification

21. Under the PSR agencies are required to set up classification review processes. This includes regular review of protective markings on information, for example, when a project has concluded or archived. Under the PSR, classified material should be declassified by the agency as soon as it no longer meets the criteria for protective marking.
22. Given the potential consequences of the disclosure of classified information, DPMC, GCSB and NZSIS consider that there is strong public and national

interest in having the agency that assigned the original protective marking be responsible for any change to the protective marking.

23. Where the Inquiry believes a protective marking may be inappropriate, the Inquiry should raise this with the responsible agency, so that the agency has an opportunity to explain the basis on which it considers that the disclosure would create a risk of prejudice and why other measures (for example, redactions, summaries of the information, declassification) would not prevent that risk. The failure to do so could inadvertently disclose information that poses a threat to national security, the public interest, or personal privacy, and could prejudice the supply of future information.

New Zealand Government Security Classifications⁴

Policy and privacy information security classifications

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 adversely affect 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 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

⁴ <https://www.protectivesecurity.govt.nz/information-security/new-zealand-government-security-classification-system/#applicationofprotectivemarkings--agencysecurityclassificationpolicy>

- 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).

National security information security classifications

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.

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.