IGIS
INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

Preliminary Inquiry into the application of national security classifications in ASIO, ASIS, ONI, ASD, AGO and DIO.

Preliminary Inquiry Report

The Hon Christopher Jessup QC

Inspector-General of Intelligence and Security

25 February 2021

IGIS
INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

Preliminary Inquiry into the application of national security classifications in ASIO, ASIS, ONI, ASD, AGO and DIO

Summary

The Office of the Inspector-General of Intelligence and Security conducted a preliminary inquiry into the application of national security classifications in the six intelligence agencies in the Inspector-General of Intelligence and Security's (IGIS) jurisdiction. As part of this preliminary inquiry IGIS staff reviewed the policy and procedures in place at each agency, conducted a survey of intelligence agency staff, and examined a selection of classified material in relation to the appropriateness of the classification decisions made.

On the basis of this preliminary inquiry, I am satisfied that there is no evidence to suggest there are systemic issues related to inappropriate classification of documents within ASIO, ASIS, ONI, ASD, AGO and DIO. Accordingly, I am satisfied that an inquiry under the *Inspector-General of Intelligence and Security Act 1986* into this matter is not required at this point.

Two recommendations have been made: the first concerns improving the currency and awareness of written guidance on national security classifications; the second concerns reviewing the suitability and frequency of training in the application of national security classifications.

As part of ongoing inspection activities of these intelligence agencies, IGIS staff will continue to review classification decisions, training and written guidance; any issues that are identified will be addressed with the relevant agency.

Background

1. In August 2020, the Parliamentary Joint Committee on Intelligence and Security's '*Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press'* recommended that the IGIS conduct a preliminary inquiry into the application of national security classifications in intelligence agencies, specifically:

> *"The Committee recommends that the Inspector-General of Intelligence and Security (IGIS), conduct a preliminary inquiry into the application of national security classifications in intelligence agencies, where such an inquiry may include:*
>
> - *Examination of a sample of classified material in relation to the appropriateness of the classification; and*
> - *Reviewing the classification procedures of intelligence agencies.*
>
> *The IGIS should advise the Committee of the outcome of any preliminary inquiry into the application of national security classifications, and to the extent possible, provide information to the public on the outcome of the inquiry. Information made available to the public may include analysis of apparent trends or culture within intelligence*

agencies in relation to applying national security classifications, or commentary on statistical trends and outcomes, as appropriate.

Additionally, any recommendations made by the IGIS to alter or improve internal practices should be prioritised by the relevant agency and reported to the Committee as part of its annual Administration and Expenditure Review"[1]

2. On 7 October 2020, the then acting Inspector-General commenced this preliminary inquiry under subsection 14(2) of the *Inspector-General of Intelligence and Security Act 1986* (the IGIS Act). In accordance with the IGIS Act, the purpose of a preliminary inquiry is to determine whether the IGIS is authorised to inquire into the matter and whether the IGIS should conduct an inquiry.

Role of the Inspector-General

3. The Inspector-General is an independent statutory office holder who is authorised to review the activities of six Australian intelligence agencies, specifically the:

   - Australian Security Intelligence Organisation (ASIO)
   - Australian Secret Intelligence Service (ASIS)
   - Australian Signals Directorate (ASD)
   - Australian Geospatial-Intelligence Organisation (AGO)
   - Defence Intelligence Organisation (DIO)
   - Office of National Intelligence (ONI)

4. By performing this role the Inspector-General assists in providing assurance that these six agencies act legally, with propriety, and that their activities are consistent with human rights. The Inspector-General discharges these responsibilities through a combination of inspections, inquiries, and investigations into complaints in accordance with the IGIS Act.

Inspections

5. Under section 9A of the IGIS Act, the functions of the Inspector-General include conducting inspections of these intelligence agencies. Regular inspections enable the Inspector-General to monitor agency activities on an ongoing basis to identify issues or concerns before they become systemic.

Inquiries

6. In accordance with Division 3 of the IGIS Act, the Inspector-General may independently initiate an inquiry in response to an identified issue or a complaint. A Minister may also refer an inquiry to the Inspector-General.

7. In conducting an inquiry the Inspector-General has significant powers which include requiring the attendance of witnesses, taking sworn evidence, and copying and retention of documents. In addition, under subsection 14(2) of the IGIS Act, the Inspector-General can conduct preliminary inquiries into matters in order to decide whether to initiate an inquiry.

---

[1] PJCIS *Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press*, August 2020, page xxii.

Complaints and public interest disclosures

8. The Inspector-General can also investigate complaints or public interest disclosures made about the six intelligence agencies within jurisdiction.

The Protective Security Policy Framework

9. The Protective Security Policy Framework (PSPF) is administered by the Attorney-General's Department (AGD)[2] and applies to non-corporate Commonwealth entities, including the six intelligence agencies within IGIS jurisdiction. The PSPF sets out government protective security policy and supports entities to implement the policy across outcomes related to security governance, information, personnel and protective security. Of specific relevance to the preliminary inquiry is the PSPF's requirement to assess sensitive and security classified information.[3]

10. To achieve this, the PSPF provides guidance on how entities can correctly assess the sensitivity or security classification of their information. This is based on the level of damage, ranging from no damage to exceptionally grave damage, that the compromise of information would be expected to cause (see Attachment A).

Preliminary inquiry approach

11. To assist in focusing the preliminary inquiry some types of material where officials have little or no discretion in the application of a security classification were excluded from the scope of this review. In particular, documents relating to warrants and authorisations which identify the target of a current intelligence operation were excluded on the basis that disclosure of such information can be expected to cause at least serious damage to the national interest, organisations or individuals. Material obtained from a foreign partner was also excluded on the basis that the original classification decision is made by a person outside IGIS jurisdiction and under the PSPF there is little scope for the classification to be altered by an Australian official.

12. In conducting the preliminary inquiry IGIS staff completed three related activities: a review of policy and procedures; a survey; and a classified material review.

Review of Policy and Procedures

13. As part of this first activity IGIS requested each agency to answer the following questions and to provide copies of associated guidance and training material:

    - What, if any, written guidance beyond the Protective Security Policy Framework (PSPF) is given to intelligence agency staff to assist them in making classification decisions?
    - What training is given to intelligence agency staff to assist them in making classification decisions (including how often)?
    - Do intelligence agencies use any form of automated or computer assisted classification (this includes a system that limits a user's choice of classification)?
    - What, if anything, has changed in intelligence agency guidance, training and systems since the addition of Division 122 to the *Criminal Code Act 1995* in 2018 (which, amongst other things, created new offences for communication or dealing with

[2] The PSPF is the responsibility of AGD, which is outside the jurisdiction of IGIS as well as the scope of this preliminary inquiry.
[3] Requirement 2 (see excerpt at Attachment A to this report).

classified information and applied strict liability to the element of classification in those offences)?

14. IGIS staff then reviewed the responses and the written guidance and training provided by each intelligence agency. The purpose of this work was to determine the effectiveness and appropriateness of these procedures and to evaluate their consistency with current PSPF and legislative requirements. The outcome of the document review also informed the conduct of the survey review and classified material review.

15. Comment: Each agency has written guidance specific to the agency on the application of national security classifications. Some documentation required updating to bring it into line with amendments to the PSPF, although for the most part this amounted to references to now defunct classifications, repealed legislation or not referencing Division 122 of the *Criminal Code Act 1995*. Relevant agencies were already aware of these issues and have advised IGIS that updated written guidance is under development.

16. Each agency also advised that it conducts training in the application of national security classifications; this training appears adequately to cover the key requirements of the PSPF in relation to classification decisions. However, IGIS staff assessed that in some cases the frequency and suitability of training was potentially inconsistent (training is discussed further below at paragraph 19).

Survey

17. In order to understand better how classification decisions are made within the six intelligence agencies, the second activity in the preliminary inquiry involved providing a survey to a selection of intelligence agency staff to complete. The answers to this survey were used by IGIS staff to understand the support provided to staff and the resources relied upon when making classification decisions.

    - Surveys were sent to agency staff covering a range of positions, levels and areas. A target of around 50 responses per agency was set, the sum of which were then assessed collectively.

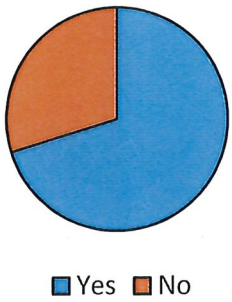
18. The survey included questions about training, reference material and other sources of guidance, perceived risk of over classification, and automation.

Questions relating to training

- Have you received formal training in person or online in relation to determining security classifications in accordance with the requirements of the PSPF?
- If yes, did this training equip you to make classification decisions in your current role?

19. Comment: The responses to these questions indicated that 70% of respondents considered the training they had been provided to be adequate (see Figure 1 below). However, noting that 30% of respondents considered their training to be inadequate, in my view, the content and frequency of training on making security classifications decisions should be regularly reviewed within each agency.

Figure 1. Did training equip you to make classification decisions in your current role?

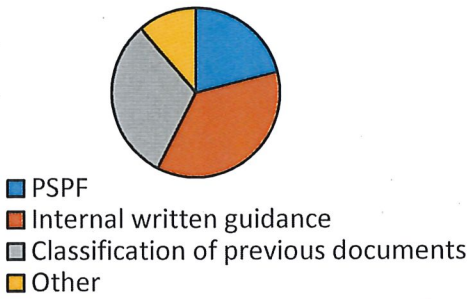


Question about documents referred to

- When making a classification decision, what documents do you refer to or otherwise rely on?

20. Comment: Responses to this question indicated a reliance on written guidance, which highlights the importance of maintaining the currency and accessibility of such guidance for making classification decisions. (See Figure 2 below)

Figure 2. When making a classification decision, what documents do you refer to or otherwise rely on?

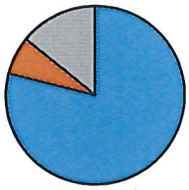


Question about adequacy of written guidance

- Do agency standard operating procedures or internal guidance documents equip you to make classification decisions in your current role?

21. Comment: In response to this question, the survey results showed that nearly 80% of respondents considered the written guidance available to them adequately equips them to make national security classification decisions. However, 20% of respondents indicated they were either not aware of such guidance or felt that it did not adequately equip them to make classifications decisions (see Figure 3 below). This suggests that the written guidance available within agencies should be more broadly promulgated and regularly reviewed to ensure it meets the needs of agency staff and addresses the relevant current legislative and policy requirements.

Figure 3. Do agency standard operating procedures or internal guidance documents equip you to make classification decisions in your current role?



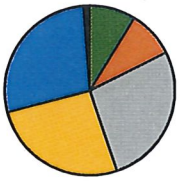
Yes No I am not aware of any written guidance

Question about assistance sought

- When making a classification decision, aside from relying on guidance documents, where else do you go for assistance?

22. Comment: The survey responses showed that nearly all respondents seek assistance from a range of areas within their agency when making classification decisions (see Figure 4 below), including about 55% who would do so from colleagues and supervisors in comparison to about 20% who would consult information security areas. This highlights the importance of all staff, regardless of their role, being adequately trained in the application of national security classifications.

Figure 4. When making a classifiction decision, aside from relying on guidance documents, where else do you go for assistance?



Agency Security Advisor
Information Security Team
Colleagues
Area of source material
Supervisor
I don't seek assistance

Question about over classification

- What types of documents do you consider to be most at risk of 'over classification'?

23. Comment: The responses to this question showed that the majority of those surveyed considered emails to be most at risk of over classification; the responses to other survey questions suggested that this risk of over classification was largely due to default or automatic classifications being applied when responding to emails (this is discussed further below).

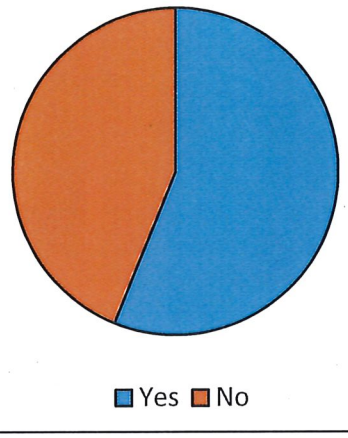
Questions about automation of classification decisions

- In making classification decisions, do you rely on automated processes or procedures to guide your decision?

- If yes, what type of automation have you relied upon?

24. Comment: A slight majority of respondents indicated they rely on automated processes or procedures to guide their decision (see Figure 5 below); for the most part this related to replying to emails where default or automatic classifications are applied in line with the classification of the original email or with the specific agency system.

Figure 5. In making classification decisions, do you rely on automated processes or procedures to guide your decision?



Classified Material Review

25. The final activity of the preliminary inquiry was a review of certain classified material held by the agencies. In conducting this review IGIS staff concentrated on whether the classification decision made in relation to the classified material was appropriate, as considered against the following criteria:

- Was the decision made in accordance with the PSPF?
- Was the decision made in accordance with internal policy and procedures?
- Was the decision consistent with the source material?
- Was the decision maker supported in making their decision?
- Overall, does the decision appear reasonable in the circumstances?

26. The classified material selected for review was based on typical IGIS inspection activities and focused on significant documents over a range of periods, including ministerial submissions, intelligence products, decision briefs and internal policies. IGIS staff also considered a selection of material generated in support of these documents, including emails and draft documents. The classification decision of each document, including the final end product, was reviewed against the above criteria. In total, over 100 classification decisions were considered.

27. Comment: This review did not identify any instances where material had been inappropriately classified. Each classification decision was made, and the resulting products classified, in accordance with the requirements of the PSPF as well as with internal policies and procedures.

Recommendations

28. I am satisfied that there is no evidence to suggest there are systemic issues related to inappropriate classification of documents within the six intelligence agencies in my jurisdiction, and that an inquiry into this matter is not required at this time. This does not mean that every classification decision made by every official in these agencies is perfect. There is always room for improvement and there are a number of staff who do not consider their training or guidance adequate or are unaware of agency guidance materials.

29. I make two recommendations on the basis of the preliminary inquiry:

Recommendation One

30. In some agencies, written guidance on national security classifications is not up to date with amendments to the PSPF and legislative provisions, and some agency staff are not aware of this written guidance. I note that during the conduct of the preliminary inquiry relevant agencies were already aware of this issue and advised my agency that updated guidance is under development.

> Recommendation 1: ASIO, ASIS, ONI, ASD, AGO and DIO should ensure that written guidance in relation to the application of national security classifications is consistent with the current Protective Security Policy Framework and relevant legislative requirements, and that agency staff are made aware of, and have access to, this guidance.

Recommendation Two

31. In some agencies, there are differences in the level and frequency of training provided to intelligence agency staff in relation to the application of national security classifications. In its August 2020 report, the PJCIS recommended that training on the application of the PSPF requirements for sensitive and classified information be made compulsory for all relevant Commonwealth officers and employees.[4] I note that the six intelligence agencies within my jurisdiction operate in a highly sensitive environment and have extensive dealings with classified material; in this context, a greater level of training is likely required than that which applies to Commonwealth agencies in general.

> Recommendation 2: ASIO, ASIS, ONI, ASD, AGO and DIO should regularly review the suitability and frequency of internal training relating to the application of national security classifications to ensure that staff are adequately supported to make classification decisions.

32. IGIS staff will monitor the implementation of these recommendations through regular inspection activities. The outcomes of IGIS inspections, inquiries and investigations will continue to be reported in the IGIS Annual Report and where possible made available on www.igis.gov.au.

---

[4] PJCIS *Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press*, August 2020, page xxi.

Attachment A

Extract of Protective Security Policy Framework[1]

Requirement 2. Assessing sensitive and security classified information

a) To decide which security classification to apply, the originator **must**:

i. assess the value, importance or sensitivity of official information by considering the potential damage to government, the national interest, organisations or individuals, that would arise if the information's confidentiality was compromised (refer to the following table), and
ii. set the security classification at the lowest reasonable level.

b) The originator must assess the information as OFFICIAL: Sensitive if:

i. a security classification does not apply, and
ii. compromise of the information's confidentiality may result in limited damage to an individual, organisation or government generally.

Protective marking	**Business impact level**	**Compromise of information confidentiality would be expected to cause:**
UNOFFICIAL	No business impact	No damage. This information does not form part of official duty.
OFFICIAL	1 Low business impact	No or insignificant damage. This is the majority of routine information.
OFFICIAL: Sensitive	2 Low to medium business impact	Limited damage to an individual, organisation or government generally if compromised.
PROTECTED	3 High business impact	**Damage** to the national interest, organisations or individuals.
SECRET	4 Extreme business impact	**Serious damage** to the national interest, organisations or individuals.
TOP SECRET	5 Catastrophic business impact	**Exceptionally grave damage** to the national interest, organisations or individuals.

[1]Protective Security Policy Framework - https://www.protectivesecurity.gov.au/