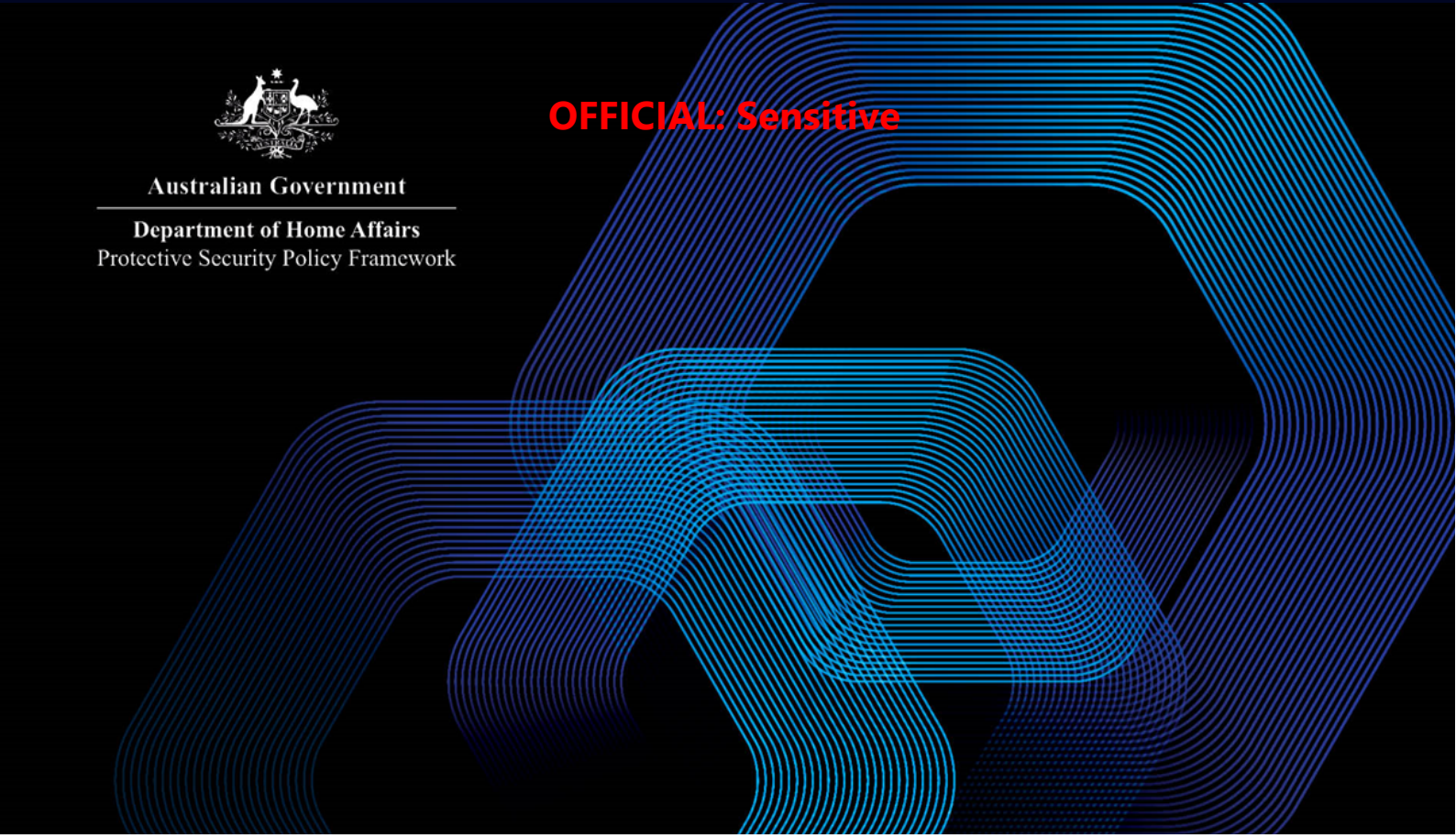
Australian Government

Department of Home Affairs

Protective Security Policy Framework



Australian Government Security Caveat Standard

Table of Contents

Purpose 3
Audience 3
Document Control 3
1. Security Caveats 4
1.1. Accountable Material 4
1.2. New or Amended Security Caveats 4
2. Security Caveat Controlling Authorities 5
3. Protective Markings 5
3.1. Security Classifications 5
3.2. Other Protective Markings 5
3.3. Information Management Markers 6
4. Applying Protective Markings 6
4.1. Paragraph Markings 6
5. National Compartments 7
5.1. New or Amended National Compartments 8
5.2. Management of National Compartments 8
5.3. Retirement of National Compartments 8
5.4. Identification of National Compartments on Identification Cards 9
6. Hierarchy of Protective Markings 9
7. Codewords 11
7.1. Entity Codewords 11
7.2. Access to and Handling of Codeword Material 11
7.3. APEX 13
7.4. ASIS Administrative Codeword 15
7.5. COMINT—Communications Intelligence 16
7.6. ECI—Exceptionally Controlled Information 17
7.7. GAMMA 18
7.8. NUCLEON 19
7.9. NUCLEON High 21
7.10. TK—Talent Keyhole 23
8. Foreign Government Markings 24
8.1. FISA—Foreign Intelligence Surveillance Act (United States) 24
8.2. HCS—HUMINT Control System (United States) 25
8.3. IMCON—Imagery Controlled (United States) 26
8.4. RSEN—Risk Sensitive (United States) 27
8.5. STRAP (United Kingdom—UK) 28

8.6. Other Foreign Government Markings (Non-Caveat) 29
8.6.1. CUI—Controlled Unclassified Information (United States) 29
8.6.2. LIMDIS—Limited Distribution (United States) 30
9. Special Handling Instructions 31
9.1. DELICATE SOURCE 31
9.2. ORCON—originator controlled 32
9.3. EXCLUSIVE FOR 33
9.4. CABINET 34
10. Releasability Caveats 35
10.1. National Intelligence Community 35
10.2. AGAO—Australian Government Access Only 36
10.3. AUSTEO—Australian Eyes Only 37
10.4. REL—Releasable To 38
11. Accountable Material 39
12. Handling, Transport and Storate Requirements 39
12.1. Courier Services 39
13. Derivative Material 39
14. Referencing Intelligence 39
14.1. Referencing by Title 39
14.2. Referencing by Number Only 40
14.3. Referencing by Entity 40
14.4. Referencing Without Attribution 40
15. Further Distribution of Intelligence 40
15.1. By Agreement 40
15.2. Sanitisation 40
15.2.1. Tearline 41
16. Classified Annex 41
17. Historical Security Caveat Register 41
17.1. NATIONAL CABINET (Historical) 41
ANNEX A 43

Purpose

The Australian Government Security Caveat Standard defines the security caveats used by the Australian Government and details the mandatory elements for handling security caveated information and accountable material, covering the following PSPF requirements.

Requirement 0063 | GOV | All entities | 31 October 2024

The Australian Government Security Caveat Standard and special Handling Requirements imposed by the Controlling Authority are applied to protect caveated information.

Requirement 0066 | GOV | All entities | 31 October 2024

Accountable material is handled in accordance with any special Handling Requirements imposed by the originator and security caveat owner detailed in the Australian Government Security Caveat Standard.

Audience

This Standard is for Non-corporate Commonwealth entities (entities) and personnel who work with security classified and caveated information and have a need-to-know.

Document Control

This document is maintained by the Department of Home Affairs on behalf of the National Intelligence and Security Subcommittee (NISS) of the Government Security Committee (GSC) and forms part of the Australian Government Protective Security Policy Framework (PSPF).

Contact the Commonwealth Security Policy section in the Department of Home Affairs via email PSPF@homeaffairs.gov.au for changes or advice.

No.	Description	Date
1.0	Initial release under PSPF Release 2024	2024-11-01
1.1	GSC agreed amendments to 'REL - Releasable To' and 'ORCON – Originator Controlled' caveats.	2024-12-12
1.2	GSC agreed to the addition of the APEX, NUCLEON and NUCLEON High codeword caveats, and to the retirement of the NATIONAL CABINET special handling instruction.	2025-03-21
1.3	GSC agreed inclusion of National Compartment arrangements	2025-06-04
1.4	GSC agreed to the addition of the INTRA national compartment, and amendments to APEX, NUCLEON, NUCLEON High, and TALENT-KEYHOLE caveats.	2025-09-25
1.5	Updates under PSPF Release 2026 – clarifying sensitive compartment information (section 7).	2026-07-01

For the current version of the Australian Government Security Caveat Standard - Classified Annex, contact the Commonwealth Security Policy section in the Department of Home Affairs via email PSPF@homeaffairs.gov.au.

Uncontrolled copies may contain out-of-date information.

1. Security Caveats

Security caveats are protective markings that further compartmentalise security-classified information. They provide a framework to ensure appropriate information handling, and strict adherence to the need-to-know principle. The need-to-know principle refers to a need to access information, based on an operational requirement.

Security Caveats impose special protections and Handling Requirements to those imposed by the security classification. For example, a security caveat may specify that information must be accessed by only those who have been briefed about its significance and need for special handling.

Security Caveats are not classifications and must appear with a security classification.

There are four categories of security caveats:

- Codewords (information that requires a compartmental briefing)
- Foreign Government Markings
- Special Handling Instructions
- Releasability Caveats.

1.1. Accountable Material

Accountable material is information that requires the strictest control over its access and movement. Accountable material includes:

- TOP SECRET information
- All codeword information
- Select special handing instruction caveats
- Any classified information designated as accountable material by the originator.

Requirement 0065 | INFO | All entities | 31 October 2024

Accountable material has page and reference numbering.

Requirement 0072 | INFO | All entities | 31 October 2024

An auditable register is maintained for TOP SECRET information and accountable material.

1.2. New or Amended Security Caveats

All requests to create a new security caveat or amend an existing security caveat in this Standard must be submitted using the request form at ANNEX A.

The Department of Home Affairs will facilitate consultation with the appropriate Commonwealth entities prior to referring to the Office of National Intelligence to facilitate consultation with the National Intelligence Community.

The requesting entity will be required to provide input to an agenda paper for the Government Security Committee's decision. Once endorsed, the Department of Home Affairs will publish the amended Caveat Standard and notify all non-corporate Commonwealth entities.

Requests for amendments to existing caveats where there is no clear ownership will be handled in the same way.

2. Security Caveat Controlling Authorities

Each security caveat is governed by a 'Controlling Authority' — the entity that originated the information marked with the security caveat and is responsible for managing and administering the security caveat.

An Australian Government entity can act as the Controlling Authority by proxy for a foreign government marking.

If an entity suspects that information marked with a security caveat is compromised, it must notify the security caveat's Controlling Authority immediately.

The following are contact details for controlling authorities for the security caveats listed in this Standard. Refer to the classified annex for additional contact details.

Table 1: Security Caveat Controlling Authorities

Entity	Telephone (unclassified)	Email (unclassified)
Australian Submarine Agency (ASA)	1800 AUKUS1 (1800 285 871)	ASA.Compartments@defence.gov.au
Australian Security Intelligence Organisation (ASIO)	02 6234 1456	product.liaison@asio.gov.au
Australian Secret Intelligence Service (ASIS)	Refer to the classified annex	
Australian Geospatial-Intelligence Organisation (AGO)	02 6127 7395	AGO.CustomerSupport@defence.gov.au
Australian Signals Directorate (ASD)	1800 744 468 or 1800 SIGINT	ASD.CustomerRelations@defence.gov.au
Defence Intelligence Organisation (DIO)	Refer to the classified annex	DIOIPC@defence.gov.au
Office of National Intelligence (ONI)	02 6144 0890	onidisseminationteam@oni.gov.au.
Department of the Prime Minister and Cabinet (PM&C)	02 6271 5111	Nationalcabinet@pmc.gov.au

3. Protective Markings

The PSPF mandates that the originator must clearly identify security classified information by using applicable protective marking, and that caveats must be marked as text and only appear in conjunction with a security classification.

3.1. Security Classifications

There are four security classifications used in the Australian Government:

- OFFICIAL: Sensitive (O:S)
- PROTECTED (P)
- SECRET (S), and
- TOP SECRET (TS).

3.2. Other Protective Markings

There are two other protective markings used in the Australian Government:

- OFFICIAL—this marking can be applied to government information from routine business
- UNOFFICIAL—this marking can be applied to information that does not form part of official duties.

These markings are not security classifications and cannot be used with security caveats.

See PSPF Release 2025 for Further Information about protective markings and security classifications.

3.3. Information Management Markers

Information management markings (IMM) are used to identify information that is subject to non-security related restrictions on access and use. Application of IMMs is optional.

See PSPF Release 2025 for details.

4. Applying Protective Markings

Applying a protective marking to information, including to attachments, in an easily identifiable way for information users (visually) and for systems (such as an entity's email gateway) helps to control information.

Examples of protective markings containing security caveats are provided throughout this Standard.

To achieve clearly identifiable protective markings, the PSPF recommends:

- Using capitals, bold text, large font and a distinctive colour (red preferred)—for example:

PROTECTED

- Placing markings at the centre top and bottom of each page.

Separating markings by a double forward slash (//) helps to clearly differentiate each marking. For the purposes of marking multiple caveats, this Standard recommends separating the elements of a caveat marking by a single space ( ) or forward slash character (/).

Requirement 0061 | INFO | All entities | 31 October 2024

Security classified information is clearly marked with the applicable security classification, and when relevant, security caveat, by using text-based markings, unless impractical for operational reasons.

Requirement 0064 | INFO | All entities | 1 July 2025

Security caveats are clearly marked as text and only appear in conjunction with a security classification.

4.1. Paragraph Markings

Marking each paragraph or section is useful but is not mandatory. The paragraph or section with the most valuable, important or sensitive information (highest classification) dictates the document's classification.

5. National Compartments

A National Compartment is a mechanism for restricting access to a defined list of individuals who have been 'briefed into the compartment'—that is, briefed on the sensitivities of that information and any special rules that may apply.

Each National Compartment has an associated codeword and/or caveats as a visual means of protecting the information contained within the National Compartment.

Each National Compartment is governed by a 'Controlling Authority' which is the originating entity of the information managed and protected within the National Compartment.

The Controlling Authority entity is responsible for:

- establishing a Compartment Briefing Officer (CBO) for their compartment with a name that aligns with the corresponding billet and differs from existing CBO roles, and
- managing and administering the National Compartment and any associated codeword and/or caveats.

All National Compartments are managed via a billet system using the NATO phonetic alphabet, whereby the next available billet is allocated by the Department of Home Affairs to successful requests. The Government Security Committee may elect to deviate from the standard naming convention where necessary.

When a National Compartment is retired, that compartments' billet will also be retired and not reserved for future use.

Entities that elect to establish internal compartments must not use the NATO phonetic alphabet to avoid any overlap in the name or cause confusion with Australian Government compartment billets.

Table 2 provides a list of the current National Compartment billets and Compartment Briefing Officers

Table 2: National Compartment Controlling Authorities

Billet	Entity	Compartment Briefing Officer	Telephone (unclassified)	Email (unclassified)
ALPHA	Reserved	Refer to the classified annex	Refer to the classified annex	Refer to the classified annex
BRAVO	Reserved	Refer to the classified annex	Refer to the classified annex	Refer to the classified annex
CHARLIE	Australian Secret Intelligence Service (ASIS)	Specialist Security Officer (SSO)	Refer to the classified annex	Refer to the classified annex
DELTA	Australian Signals Directorate (ASD)	Communications Intelligence Security Officers (COMSO)	1800 744 468 or 1800 SIGINT	ASD.CustomerRelations@defence.gov.au
ECHO	Australian Geospatial-Intelligence Organisation (AGO)	Refer to the classified annex	02 6127 7395	AGO.CustomerSupport@defence.gov.au
FOXTROT	Retired	Retired	Retired	Retired
GAMMA	Australian Signals Directorate (ASD)	Refer to the classified annex	1800 744 468 or 1800 SIGINT	ASD.CustomerRelations@defence.gov.au
HOTEL	Reserved	Refer to the classified annex	Refer to the classified annex	Refer to the classified annex

Billet	Entity	Compartment Briefing Officer	Telephone (unclassified)	Email (unclassified)
INTRA	Australian Submarine Agency	INTRA Control Officer (ICO)	1800 285 871 or 1800 AUKUS1	ASA.Compartments@defence.gov.au

5.1. New or Amended National Compartments

When requesting the establishment of a National Compartment or requesting to amend an existing National Compartment, the Controlling Authority must:

- Complete and submit the request form at ANNEX A to the Department of Home Affairs.

  Note: Entities that elect to establish entity-specific compartments are not National Compartments and are therefore not included in this Standard. An entity may seek to elevate its entity-specific compartment to a National Compartment using the request form at ANNEX A.
- Notify the Accountable Authority, Chief Security Officer and Chief Information Security Officer once approved.
- Brief the Accountable Authority, and Chief Security Officer and Chief Information Security Officer where appropriate, into the National Compartment and advise the following details:
  - date of establishment
  - Controlling Authority
  - all delegates listed to act on behalf of the Controlling Authority, and
  - the arrangements for managing the National Compartment, including the name of the Compartment Briefing Officer.

5.2. Management of National Compartments

The Controlling Authority is responsible for the ongoing management of its National Compartment, including the briefing requirements associated with its National Compartment, and incident response, remediation and reporting required by the PSPF.

Unauthorised access to a National Compartment constitutes a significant security incident and must be treated as an incident requiring remediation and reporting.

The briefing requirements should include:

- eligibility requirements (and any allowed exceptions)
- briefing content and process
- refresher briefing timeframes
- record keeping and incident management arrangements
- transfer of briefings, and
- debriefing procedures.

5.3. Retirement of National Compartments

When retiring a National Compartment, the Controlling Authority must:

- Notify the Accountable Authority, Chief Security Officer and Chief Information Security Officer prior to the retirement.

- Complete and submit the request form at ANNEX A to the Department of Home Affairs prior to retirement.
- Debrief all individuals from the compartment prior to retirement.

5.4. Identification of National Compartments on Identification Cards

See Classified Annex for information on displaying briefings into National Compartments on identification cards.

6. Hierarchy of Protective Markings

Under the PSPF, the order of precedence or hierarchy for protective markings is:

1. Classification
2. National Compartment (not visually identified on documents or correspondence)
3. Caveats, in the following order:

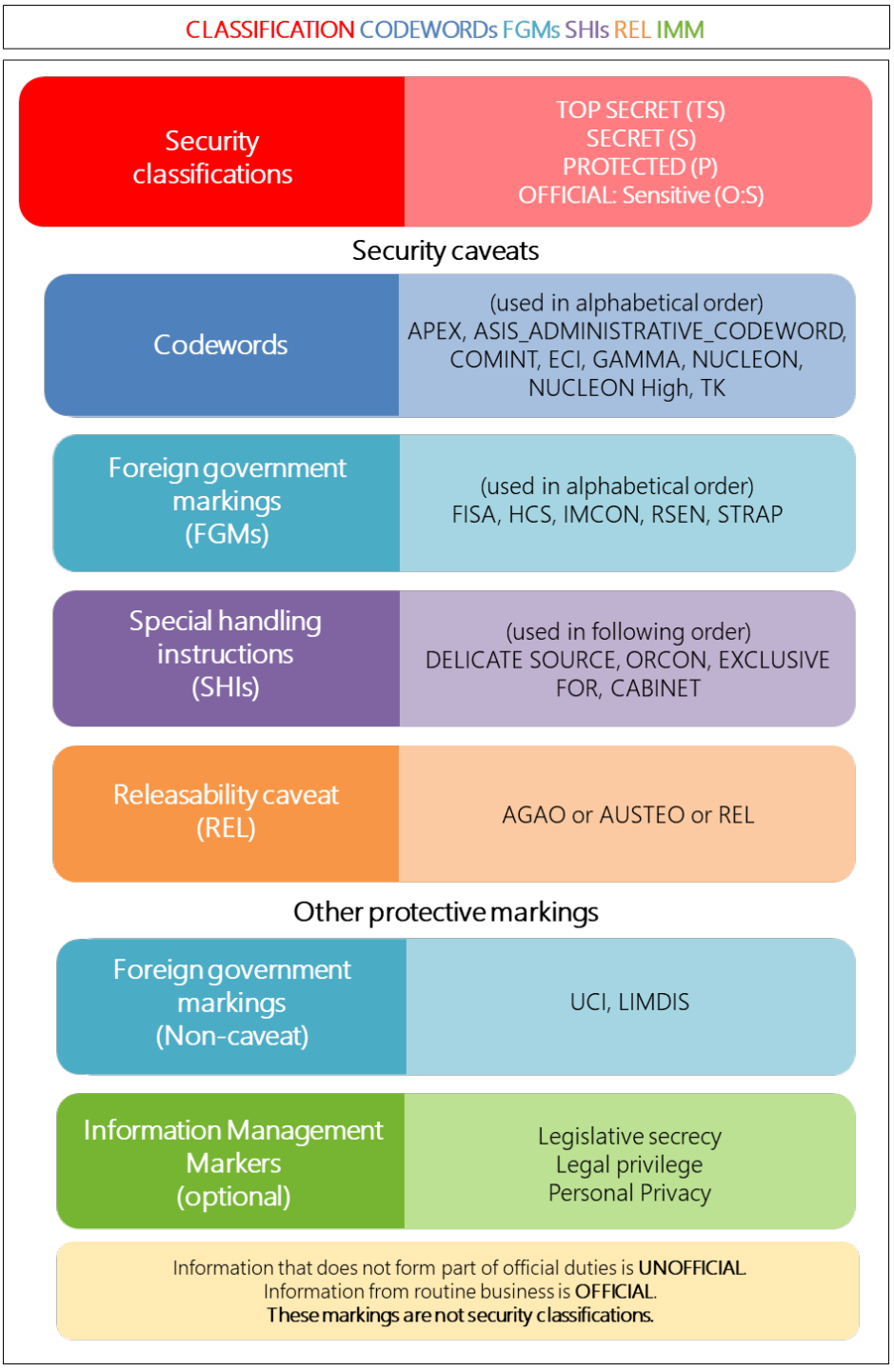
- Codewords
- Foreign Government Marking
- Special Handling Instructions, and
- Releasability Caveats

4. (Optional) Information Management Markers.

NOTE: the above guidance is distinct from the standardised format for protective markings on emails exchanged in and between Australian Government entities, detailed in the Australian Government Email protective marking standard (EPMS).

Protective marking elements of caveated information adhere to the following hierarchy and order—
the elements have been colour-coded for clarity only.

Figure 1: Hierarchy of elements in protective markings of caveated information



This hierarchy and order is illustrated further by the following examples—colour-coded for clarity only:

TOP SECRET COMINT FISA HCS DELICATE SOURCE ORCON REL AUS/CAN/GBR/GBR/NZL/USA
SECRET APEX ASIS_ADMINISTRATIVE_CODEWORD COMINT ORCON AGAO Legislative secrecy
PROTECTED AUSTEO NUCLEON High Legal privilege
OFFICIAL: Sensitive NUCLEON Personal Privacy

7. Codewords

A codeword indicates that sensitivity of the information it covers—called 'codeword material'—requires additional protection to the security classification.

Each codeword identifies a special need-to-know compartment. A compartment is a mechanism for restricting access to a defined list of individuals who have been 'briefed into the compartment'—that is, briefed on sensitivities of that information and any special rules that may apply.

A codeword conceals the meaning or source it covers and the codeword itself (as opposed to its meaning or source) is unclassified. However, material containing a codeword and all associated information divulging its meaning or source must be protectively marked. Similarly, a codeword used frequently or distributed widely could be compromised over time, and the Controlling Authority should consider changing it.

The tables in this section define codewords commonly used in the Australian Government.

Sensitive Compartment Information (SCI) consists of security classified information baring the following security caveats:

- COMINT—Communications Intelligence
- ECI—Exceptionally Controlled Information
- GAMMA (including sub-compartments)
- TK—Talent Keyhole

PSPF Requirement 0199 mandates that SCI must be stored, process, handled and discussed within Sensitive Compartmented Information Facilities (SCIFs).

7.1. Entity Codewords

Entities may define their own codewords. When an entity introduces a new codeword, they become the Controlling Authority for that codeword and must inform recipient entities how material with the new codeword should be handled.

A codeword and its meaning must not relate to the source, subject or purpose of the information it covers. In general, codewords should:

- be one or two words
- not have been previously used
- not incorporate numbers
- not be derogatory
- not be culturally insensitive, and
- not be an Indigenous word.

An entity that defines its own codewords must maintain a central list of its codewords or seek approval to include the codeword in this Standard.

7.2. Access to and Handling of Codeword Material

Access to codeword material by a designated person is granted on a need-to-know basis and must be justified by their line manager and approved by the appropriate delegate.

On advice from the line manager or appropriate delegate, the COMSO will arrange for the designated person to be briefed by the Controlling Authority of the codeword. See the Australian SIGINT Handling Standards for further details on the COMSO's role and responsibilities.

When a designated person no longer requires access to codeword material, their line manager must advise the COMSO, who will arrange for the designated person to be de-briefed by the Controlling Authority of the codeword.

The COMSO will ensure all requests for codeword briefings and de-briefings are justified, approved and recorded both internally and with the Controlling Authority of the codeword.

Entities must ensure that information management/registry staff and personal assistants are authorised and briefed to access and handle codeword material required in the course of their duties.

7.3. APEX

Controlling Authority	Australian Submarine Agency (ASA)
Access Requirements	A minimum Negative Vetting Level 1 security clearance and a Nuclear Mindset Suitability Assessment (NMSA) (Full) is required for regular, ongoing access to, or for the generation of, APEX material. The need-to-know requirements for this caveat is managed through the approval process for briefing into the ASA Naval Nuclear Propulsion Information (NNPI) Level 3 Compartment.
Briefing Requirements	INTRA ASA NNPI Level 3 Compartment Briefing, administered by the ASA Compartment Control Authority or a delegate on behalf of the Compartment Sponsor.
Security Classifications	SECRET/TOP SECRET **Note**: APEX material must be stored, processed and transmitted on systems approved for NNPI. System approval is managed through ASA's Chief Information Security Officer.
Definition	NNPI including ATOMIC information and Restricted Data as defined in the AUKUS Naval Nuclear Propulsion Agreement (ANNPA) that is sensitive information related to the design, operation and maintenance of naval nuclear propulsion systems that use special nuclear material in the production of energy. APEX information strictly excludes the design, manufacture, or utilisation of atomic weapons, all of which are outside the scope of the ANNPA. APEX information replaces SOUTHERN APEX as identified in ANNPA. **Note**: Additional information can be found in the ASA NNPI Policy.
Application	Header/footer examples: SECRET APEX SECRET//APEX TOP SECRET APEX TOP SECRET//APEX
Handling Requirements	**Electronic handling**: APEX material must be stored, processed and transmitted electronically only on accredited NNPI systems. **Physical handling**: APEX material must be physically handled and protected as a minimum of SECRET classified information, APEX material must be passed to confirmed ASA NNPI Level 3 Compartment briefed people only. **Storage**: APEX material must be stored and processed within a minimum Security Zone 4 (as defined in the PSPF) unless otherwise advised. Refer to the ASA NNPI Policy for specific requirements. Contact ASA for further details.
Warning Notice	N/A
Sanitisation	For all requests, contact the Controlling Authority (ASA) for approval through the ASA Compartment Control Authority.
Referencing	Refer to ASA Compartment Control Authority.
Destruction	**Electronic:** Contact the Controlling Authority (ASA) for advice through the ASA Compartment Control Authority. **Physical:** APEX information classified SECRET must be destroyed to a minimum SECRET standard as outlined in the PSPF. TOP SECRET APEX information must be destroyed in accordance with TOP SECRET requirements as outlined in the PSPF. Refer to the ASA NNPI Policy for specific requirements. Contact ASA for further details.

Controlling Authority	Australian Submarine Agency (ASA)
Further Information	Contact the Controlling Authority (ASA Compartment Control Authority)—see Security Caveat Controlling Authorities.

7.4. ASIS Administrative Codeword

Controlling Authority	Australian Secret Intelligence Service (ASIS)
Access Requirements	Minimum prerequisite: Negative Vetting 1 (NV1) security clearance A Positive Vetting (PV) or TOP SECRET-Privileged Access (TS-PA) security clearance is required for regular, ongoing access.
Briefing Requirements	CHARLIE briefing, administered by ASIS or delegated agency special security officer (SSO)
Security Classifications	SECRET/TOP SECRET **Whatever its classification, ASIS administrative codeword material must be stored, processed and transmitted on TOP SECRET systems only.**
Definition	Refer to the classified annex of this Standard for Further Information.
Application	Header/footer examples: SECRET ASIS_ADMINISTRATIVE_CODEWORD SECRET//ASIS_ADMINISTRATIVE_CODEWORD
Handling Requirements	**Must be treated as accountable material.** Refer to the classified annex of this Standard for Further Information. **Electronic handling**: Material must be stored, processed and transmitted electronically on a TOP SECRET–accredited sensitive compartmented information (SCI) system. **Physical handling**: In addition to the handling instructions for the respective classification (SECRET or TOP SECRET), material must be passed to confirmed CHARLIE-briefed people only. **Storage**: Material must be stored and processed within a Security Zone 5 (as defined in the PSPF) unless otherwise advised. Consult ASIS for details. **Legal**: ASIS-generated material is exempt from certain federal Acts (e.g. the Privacy Act) and certain sections of other federal Acts (e.g. the Archives Act and the *Freedom of Information Act 1982*).
Warning Notice	N/A
Sanitisation	Contact the Controlling Authority (ASIS) for approval.
Referencing	Refer to Referencing Intelligence.
Destruction	**Electronic**: See the *Information security manual* for further details. **Physical**: According to the PSPF instructions for the security classification of the material.
Further Information	Contact the Controlling Authority (ASIS)—see Security Caveat Controlling Authorities.

7.5. COMINT—Communications Intelligence

Controlling Authority	Australian Signals Directorate (ASD)
Access Requirements	A Positive Vetting (PV) or TOP SECRET-Privileged Access (TS-PA) security clearance is required for access to COMINT material. A Negative Vetting 2 (NV2) security clearance allows limited access to ASD's COMINT reports on a case-by-case basis, subject to ASD approval.
Briefing Requirements	DELTA briefing, administered by an authorised delegate of Director-General ASD
Security Classifications	SECRET/TOP SECRET **Whatever its classification, COMINT material must only be stored, processed and transmitted on TOP SECRET systems.**
Definition	Details of the application of the COMINT caveat are classified; however, ASD's intelligence functions are outlined in unclassified terms in Section 7 of the *Intelligence Services Act 2001*. Foreign markings equivalent to COMINT are SI or Special Intelligence (USA) and STRAP (UK), see Foreign Government Markings. **Previously related markings**: COMINT has replaced other caveats including UMBRA, MORAY, SPOKE and HVCCO. These legacy caveats should no longer be used.
Application	Header/footer examples: TOP SECRET COMINT REL AUS/CAN/GBR/NZL/USA TOP SECRET//COMINT//REL AUS/CAN/GBR/NZL/USA
Handling Requirements	**Must be treated as accountable material.** COMINT Handling Requirements are detailed in ASD's Australian SIGINT Handling Standards (ASHS) and must be adhered to. The ASHS are available from agency COMSOs.
Warning Notice	ASD applies the following mandatory Warning Notice to its published COMINT products: This information has been communicated for intelligence purposes only. It may be used to develop potential investigative leads but must not be used in any legal proceedings or in response to any requirement to provide the information (e.g. under subpoena), without the approval of the Australian Signals Directorate (ASD). It must not be re-classified, downgraded or further released without ASD approval. This document, and any information extracted from it, is exempt under the *Freedom of Information Act 1982*. Other agencies may include a Warning Notice that incorporates similar restrictions.
Sanitisation	Contact the Controlling Authority (ASD) for approval.
Referencing	Refer to Referencing Intelligence. Document or serial numbers should be used to reference ASD COMINT products in derivative material. Where derivative material bears the same or higher classification and protective markings as the original, and is not marked ORCON or GAMMA, ASD approval is not required to reference or draw on COMINT.
Destruction	**Electronic**: See the *Information security manual* for further details. **Physical**: See the *Australian SIGINT Handling Standards (ASHS)* or seek guidance from ASD. The ASHS are available from agency COMSOs.
Further Information	Contact the Controlling Authority (ASD)—see Security Caveat Controlling Authorities.

7.6. ECI—Exceptionally Controlled Information

Controlling Authority	Australian Security Intelligence Organisation (ASIO) Australian Secret Intelligence Service (ASIS) Australian Geospatial-Intelligence Organisation (AGO) Australian Signals Directorate (ASD)
Access Requirements	Minimum prerequisite: A Positive Vetting (PV) or TOP SECRET-Privileged Access (TS-PA) security clearance. ECI from ASIS also requires a CHARLIE briefing. ECI from ASD also requires a DELTA briefing
Briefing Requirements	Each ECI has specific briefing requirements. A briefing can be provided only by the respective compartment controller or owner (see below).
Security Classification	Minimum TOP SECRET
Definition	ECIs are specific compartments generated to protect information or operations where the application of the need-to-know principle is critical. Each ECI compartment will have its own specific definition (usually itself highly classified) that details the type of information or specific operation it covers. **Previously related markings**: The ECI caveat replaces the Very Restricted Knowledge (VRK) caveat previously generated by SIGINT agencies.
Application	Header/footer examples: TOP SECRET COMINT ECI POTTER REL AUS/GBR TOP SECRET//COMINT/ECI POTTER/REL AUS/GBR
Handling Requirements	**Must be treated as accountable material.** **Electronic handling**: Generally only processed on TOP SECRET–accredited systems but with additional controls (specified by the originating agency) that restrict access to specific people while the data is at rest or in transit. **Physical handling**: In accordance with TOP SECRET codeword material, ECI material is passed via safe hand only, to appropriately briefed people only. **Storage**: ECI material must be stored within a Security Zone 5 (as defined in the PSPF) and must be physically separated from non-ECI material. It must not be archived on agency files. **Creation:** An ECI compartment should be created only where there is no appropriate protective marking that has satisfactory controls when the need-to-know principle is applied. An ECI compartment is created by clearly defining the scope of the information or operation to be compartmented and assigning an owner (usually an SES-equivalent) and a controller (a senior or executive level APS). **Responsibilities**: The owner is responsible for overall access to the compartment. The controller is responsible for the administration of the compartment, including briefing people in and debriefing people out, and maintaining the list of people who have been briefed. People no longer requiring access to an ECI must be debriefed out of the respective compartment at the earliest opportunity. **Legal**: The use of an ECI does not negate the responsibility of agencies to comply with any federal Act, bilateral agreement or the direction of a relative authority (e.g. Inspector-General of Intelligence and Security (IGIS), Commonwealth Ombudsman). This information provides the minimum standard for handling ECI material. In all cases, further guidance from the ECI owner should be sought.
Warning Notice	N/A
Sanitisation	Approval must be obtained from the originating agency.
Referencing	Refer to Referencing Intelligence.
Destruction	**Electronic**: See the *Information security manual* for further details. **Physical**: According to the PSPF instructions for material marked TOP SECRET codeword
Further Information	Contact the Controlling Authority—see Security Caveat Controlling Authorities.

7.7. GAMMA

Controlling Authority	Australian Signals Directorate (ASD)
Access Requirements	Minimum prerequisite: A Positive Vetting (PV) or TOP SECRET-Privileged Access (TS-PA) security clearance **and** a DELTA briefing
Briefing Requirements	GAMMA briefing administered by an authorised delegate of Director-General ASD
Security Classifications	Minimum TOP SECRET COMINT ORCON
Definition	Particularly sensitive COMINT which requires additional protection to that prescribed for COMINT caveat.
Application	Header/footer examples: TOP SECRET COMINT GAMMA ORCON REL AUS/CAN/GBR/NZL/USA TOP SECRET//COMINT/GAMMA/ORCON/REL AUS/CAN/GBR/NZL/USA
Handling Requirements	**Must be treated as accountable material.** **Electronic handling**: GAMMA must only be stored, processed and transmitted on TOP SECRET COMINT GAMMA-accredited systems, with additional controls to restrict access while data is at rest or in transit such as an Exclusive Community of Interest (ECOI) on a system accredited by ASD to carry GAMMA material. **GAMMA Handling Requirements:** are detailed in supplementary policies to ASD's SIGINT Handling Standards (ASHS), and must be adhered to. The ASHS and its supplementary documents are available from agency COMSOs.
Warning Notice	ASD applies the following mandatory Warning Notice to its published GAMMA products: This is a highly-sensitive GAMMA report. It is provided for GAMMA-briefed personnel only who have a clear need-to-know for the particular report subject.
Sanitisation	Appropriately classified requests for sanitisation of GAMMA material should be sent to ASD customer relations via AICNet at asd.customerrelations@defence.gov.au.
Referencing	Referencing and use of GAMMA information in derivative material requires prior approval from ASD. See also the corresponding guidance for COMINT. The Warning Notice (above) must be applied to derivative material that references GAMMA information.
Destruction	**Electronic**: See the *Information Security Manual* for further details. **Physical**: See the ASHS and supplementary policies, or seek guidance from ASD. The ASHS and its supplementary documents are available from agency COMSOs.
Further Information	Contact the Controlling Authority (ASD)—see Security Caveat Controlling Authorities.

7.8. NUCLEON

Controlling Authority	Australian Submarine Agency (ASA)
Access Requirements	An Australian Baseline security clearance is required for regular, ongoing access to, or for the generation of, NUCLEON material. The need-to-know requirements for this caveat is managed through the approval process for briefing into the ASA Naval Nuclear Propulsion Information (NNPI) Level 1 Compartment.
Briefing Requirements	INTRA ASA NNPI Level 1 Compartment Briefing, administered by the ASA Compartment Control Authority or a delegate on behalf of the Compartment Sponsor.
Security Classifications	OFFICIAL: Sensitive/PROTECTED/SECRET/TOP SECRET **Note**: NUCLEON material must be stored, processed and transmitted on systems approved for NNPI. System approval is managed through ASA's Chief Information Security Officer.
Definition	All NNPI as defined in the ANNPA that is: 1. Exclusively derived from the United States at the Controlled Unclassified Information level, or, 2. Generated by Australia for bilateral exchange with the US at the OFFICIAL: Sensitive level. **Note 1**: OFFICIAL: Sensitive NUCLEON information shared with the United Kingdom is handled as UK OFFICIAL-SENSITIVE Naval Nuclear Propulsion Program Information (UK OS NNPPI) with the attendant higher personnel security requirements applied. If returned to Australia, this information must be handled as OFFICIAL: Sensitive NUCLEON High. **Note 2**: Documents containing information classified up to and including TOP SECRET may include NNPI up to OFFICIAL: Sensitive NUCLEON caveated information. E.g. a SECRET AGAO document which includes O:S NUCLEON NNPI. **Note 3**: Additional information can be found in the ASA NNPI Policy.
Application	Header/footer examples: OFFICIAL: Sensitive NUCLEON OFFICIAL: Sensitive//NUCLEON PROTECTED NUCLEON PROTECTED//NUCLEON SECRET NUCLEON SECRET//NUCLEON TOP SECRET NUCLEON TOP SECRET//NUCLEON
Handling Requirements	**Electronic handling**: NUCLEON material must be stored, processed and transmitted electronically only on accredited NNPI systems. **Physical handling**: NUCLEON material must be physically handled and protected as a minimum of PROTECTED classified information, NUCLEON material must be passed to confirmed ASA NNPI Level 1 Compartment briefed people only. **Storage**: NUCLEON material must be stored and processed within a minimum Security Zone 2 (as defined in the PSPF) unless otherwise advised. Refer to the ASA NNPI Policy for specific requirements. Contact ASA for further details.
Warning Notice	N/A

Controlling Authority	Australian Submarine Agency (ASA)
Sanitisation	For all requests, contact the Controlling Authority (ASA) for approval through the ASA Compartment Control Authority.
Referencing	Refer to ASA Compartment Control Authority.
Destruction	**Electronic:** Contact the Controlling Authority (ASA) for advice through the ASA Compartment Control Authority. **Physical:** All NUCLEON information must be destroyed to a SECRET standard as outlined in the PSPF. Refer to the ASA NNPI Policy for specific requirements. Contact ASA for further details.
Further Information	Contact the Controlling Authority (ASA Compartment Control Authority)—see Security Caveat Controlling Authorities.

7.9. NUCLEON High

Controlling Authority	Australian Submarine Agency through the ASA Compartment Control Authority.
Access Requirements	A minimum of a Negative Vetting Level 1 security clearance and a Nuclear Mindset Suitability Assessment (NMSA) is required for regular, ongoing access to, or for the generation of, NUCLEON High material. The need-to-know requirements for this caveat is managed through the approval process for briefing into the ASA Naval Nuclear Propulsion Information (NNPI) Level 2 Compartment.
Briefing Requirements	INTRA ASA NNPI Level 2 Compartment Briefing, administered by the ASA Compartment Control Authority or a delegate on behalf of the Compartment Sponsor (See section 5.5 INTRA).
Security Classifications	OFFICIAL: Sensitive/PROTECTED/SECRET/TOP SECRET **Note**: NUCLEON High material must be stored, processed and transmitted on systems approved for NNPI. System approval is managed through ASA's Chief Information Security Officer.
Definition	All NNPI as defined in the ANNPA that is: 1. Exclusively derived from United Kingdom NNPI, or, 2. Generated by Australia for bilateral exchange with the UK at the OFFICIAL: Sensitive level or above, or, 3. Generated by Australia for trilateral exchange at the OFFICIAL: Sensitive level or above, or 4. Generated by Australia for sovereign use, where the originator requires recipients to be briefed into the Level 2 or higher compartment. **Note**: Additional information can be found in the ASA NNPI Policy.
Application	Header/footer examples: OFFICIAL: Sensitive NUCLEON High OFFICIAL: Sensitive//NUCLEON High PROTECTED NUCLEON High PROTECTED//NUCLEON High SECRET NUCLEON High SECRET//NUCLEON High TOP SECRET NUCLEON High TOP SECRET//NUCLEON High
Handling Requirements	**Electronic handling:** NUCLEON High material must be stored, processed and transmitted electronically only on accredited NNPI systems. **Physical handling:** NUCLEON High material must be physically handled and protected as outlined in the ASA NNPI Policy, NUCLEON High material must be passed to confirmed ASA NNPI Level 2 Compartment briefed people only. **Storage:** NUCLEON High material must be stored and processed within a minimum Security Zone 2 (as defined in the PSPF) unless otherwise advised and outlined in the ASA NNPI Policy. Refer to the ASA NNPI Policy for specific requirements. Contact ASA for further details.
Warning Notice	N/A

Controlling Authority	Australian Submarine Agency through the ASA Compartment Control Authority.
Sanitisation	For all requests, contact the Controlling Authority (ASA) for approval through the ASA Compartment Control Authority.
Referencing	Refer to ASA Compartment Control Authority.
Destruction	**Electronic:** Contact the Controlling Authority (ASA) for advice through the ASA Compartment Control Authority. **Physical:** NUCLEON High information classified SECRET or below must be destroyed to a minimum SECRET standard as outlined in the PSPF. TOP SECRET NUCLEON High information must be destroyed in accordance with TOP SECRET requirements as outlined in the PSPF. Refer to the ASA NNPI Policy for specific requirements. Contact ASA for further details.
Further Information	Contact the Controlling Authority (ASA Compartment Control Authority)—see Security Caveat Controlling Authorities.

7.10. TK—Talent Keyhole

Controlling Authority	Australian Geospatial-Intelligence Organisation (AGO)
Access Requirements	Minimum prerequisite: A Positive Vetting (PV) or TOP SECRET-Privileged Access (TS-PA) security clearance
Briefing Requirements	ECHO briefing administered by Defence Intelligence Security
Security Classification	SECRET / TOP SECRET
Definition	The definition and use of the TK caveat is classified TOP SECRET. Contact AGO for Further Information. **Previously related markings**: The TK caveat replaces BYEMAN.
Application	Header/footer examples: SECRET TK REL AUS/GBR SECRET//TK/REL AUS/GBR TOP SECRET TK REL AUS/GBR TOP SECRET//TK/REL AUS/GBR
Handling Requirements	**Must be treated as accountable material.** **Electronic handling**: Regardless of classification, TK material must be stored, processed and transmitted only on TOP SECRET TK-accredited systems. **Physical handling**: In addition to the handling instructions for the respective classification (SECRET or TOP SECRET), TK material must be passed to confirmed ECHO-briefed people only. **Storage**: TK material must be stored and processed within a Security Zone 5 (as defined in the PSPF). Must not be stored on agency files or archived. Contact Defence Intelligence Security for further details. In accordance with the security classification of material, written approval must be obtained from the controlling agency before TK material can be manually transmitted by either an endorsed safe-hand (person to person) carrier or an endorsed overnight courier. All requests for approval must be lodged in writing to Defence Intelligence Security. All requests will be assessed on a case-by-case basis.
Warning Notice	This Warning Notice is mandatory: This document contains references to sensitive analytical techniques (sensitive TK information). Further re-use or dissemination of this information beyond AUS, CAN, GBR, NZL or USA requires the written approval of the Australian Geospatial-Intelligence Organisation (AGO).
Sanitisation	Contact the Controlling Authority (AGO) for approval.
Referencing	Refer to Referencing Intelligence.
Destruction	**Electronic handling**: See the *Information security manual* for further details. **Physical**: Seek guidance from Defence Intelligence Security.
Further Information	Contact the Controlling Authority (AGO)—see Security Caveat Controlling Authorities.
Controlling Authority	Australian Geospatial-Intelligence Organisation (AGO)
Access Requirements	Minimum prerequisite: A Positive Vetting (PV) or TOP SECRET-Privileged Access (TS-PA) security clearance
Briefing Requirements	ECHO briefing administered by Defence Intelligence Security

8. Foreign Government Markings

This section defines foreign government markings (FGMs) and specifies how Australian entities should treat them.

Each FGM has one or more Australian agencies that act as controlling authorities by proxy and administer the FGM in Australia.

FGMs are applied to material created by Australian entities from foreign source information to maintain protection:

- at least equivalent to that required by the foreign government providing the source material; and
- if the material re-enters a foreign government system.

There are two FGMs that are not caveats as they are not applied to security classified information. These are described at Other Foreign Government Markings (Non-Caveat).

8.1. FISA—Foreign Intelligence Surveillance Act (United States)

Refer to the classified annex of this Standard for information.

8.2. HCS—HUMINT Control System (United States)

Controlling Authority	Australian Secret Intelligence Service (ASIS) by proxy
Access Requirements	A Positive Vetting (PV) or TOP SECRET-Privileged Access (TS-PA) security clearance is required for regular, ongoing access to, or for the generation of, HCS material. In limited circumstances a Negative Vetting 2 (NV2) security clearance may suffice for irregular and/or a finite period of access. Prior approval must be obtained from ASIS.
Briefing Requirements	CHARLIE briefing administered by ASIS or a delegated agency special security officer (SSO)
Security Classifications	SECRET/TOP SECRET Whatever its classification, HCS material must be stored, processed and transmitted on TOP SECRET systems only
Definition	HUMINT Control System (HCS) is a United States reporting compartment. Refer to the classified annex of this Standard for Further Information.
Application	Header/footer examples: TOP SECRET HCS TOP SECRET//HCS
Handling Requirements	**Must be treated as accountable material.** **Electronic handling**: HCS material must be stored, processed and transmitted electronically on TOP SECRET–accredited sensitive compartmented information (SCI) systems. **Physical handling**: In addition to the handling instructions for the respective classification (SECRET or TOP SECRET), HCS material must be passed to confirmed CHARLIE-briefed people only. **Storage**: HCS material must be stored and processed within a Security Zone 5 (as defined in the PSPF) unless otherwise advised. Contact ASIS for further details.
Warning Notice	This Warning Notice is **mandatory**: Some of the information contained in this report is based on US HUMINT Control System (HCS)-derived reporting. • US recipients must retain within HCS channels. This information is provided only for intelligence purposes in an effort to develop potential investigative leads. It cannot be used in affidavits, court proceedings or subpoenas or for other legal or judicial purposes. • Australian recipients must store, process and transmit only on TOP SECRET COMINT accredited systems. In addition, HCS-derived reporting is to be passed to confirmed CHARLIE-briefed people only.
Sanitisation	For all requests, contact the Controlling Authority (ASIS) for approval. Refer to the classified annex of this Standard for Further Information.
Referencing	Refer to Referencing Intelligence. HCS-derived reporting including summaries, assessments and briefings must be classified TOP SECRET and include the mandatory Warning Notice (above).
Destruction	**Electronic**: See the *Information security manual* for further details. **Physical**: According to the PSPF instructions for the security classification of the material
Further Information	Contact the Controlling Authority (ASIS)—see Security Caveat Controlling Authorities.

8.3. IMCON—Imagery Controlled (United States)

Controlling Authority	Australian Geospatial-Intelligence Organisation (AGO) by proxy
Access Requirements	Minimum prerequisite: Negative Vetting 2 (NV2) security clearance IMCON material can be distributed to Five-Eyes intelligence agencies and suitably cleared AUS/CAN/GBR/NZL/USA personnel without receiving prior approval from AGO as the originating agency. **Further distribution to other foreign entities is prohibited without receiving prior approval from AGO.**
Briefing Requirements	N/A
Security Classifications	SECRET/TOP SECRET **Whatever its classification, IMCON material must be stored, processed and transmitted on TOP SECRET systems only.**
Definition	This caveat is applied to SECRET-level Sensitive Analytical Techniques (SATs) that have been approved by the Sensitive Analytical Techniques Panel (SATP). SATs are sensitive imagery signatures that can be classified, with prior SATP approval, at either the SECRET//IMCON or TOP SECRET//TK/RSEN level. IMCON is used to protect sources and analytic methods associated with the geospatial intelligence discipline that are particularly vulnerable to countermeasures and, if disclosed or released, could nullify or measurably reduce the effectiveness of those methodologies.
Application	Header/footer examples: TOP SECRET IMCON TOP SECRET//IMCON
Handling Requirements	**Must be treated as accountable material.** **Electronic handling**: IMCON material must be stored, processed and transmitted electronically on TOP SECRET–accredited systems only. AGO cable reports published with IMCON handling notices may be sent on the ASCON system only. **Physical handling and storage**: As per security classification **Storage**: IMCON material must be stored and processed within a Security Zone 5 (as defined in the PSPF) unless otherwise advised.
Warning Notice	This Warning Notice is mandatory: OFFICIAL: Sensitive IMCON WARNING: Imagery Controlled (IMCON) information is derived from sensitive imagery analytical techniques. This handling instruction protects and emphasises the sensitivity of certain analytical techniques, as well as the products and intelligence associated with these capabilities. IMCON information must not be distributed on SECRET networks. Contact the Controlling Authority (AGO) for Further Information.
Sanitisation	Contact the Controlling Authority (AGO) for approval.
Referencing	Refer to Referencing Intelligence.
Destruction	**Electronic**: See the *Information security manual* for further details. **Physical**: According to the PSPF instructions for material classified TOP SECRET.
Further Information	Contact the Controlling Authority (AGO)—see Security Caveat Controlling Authorities.

8.4. RSEN—Risk Sensitive (United States)

Controlling Authority	Australian Geospatial-Intelligence Organisation (AGO) by proxy
Access Requirements	Minimum prerequisite: Negative Vetting 1 (NV1) security clearance RSEN material can be distributed to Five-Eyes intelligence agencies and suitably cleared AUS/CAN/GBR/NZL/USA personnel without prior approval from AGO as the originating agency. **Further dissemination to other foreign entities is prohibited without prior approval from AGO.**
Briefing Requirements	N/A
Security Classifications	SECRET/TOP SECRET
Definition	RSEN is used to protect especially sensitive imaging capabilities and exploitation techniques. This marking must only be used with TOP SECRET or SECRET information. This marking may be used with the TK caveat.
Application	Header/footer examples: TOP SECRET RSEN TOP SECRET//RSEN
Handling Requirements	**Electronic handling**: TOP SECRET RSEN material must be stored, processed and transmitted electronically on TOP SECRET–accredited systems only. SECRET RSEN material must be stored, processed and transmitted electronically on TOP SECRET–accredited or SECRET-accredited systems only. SECRET RSEN product may be published or transferred to AICNet, SIREN, JISS, Stone Ghost, the Defence Secret Network and Satin High. AGO cable reports with RSEN handling notices must be sent on the ASCON system only. **Physical handling**: As per security classification **Storage**: As per security classification
Warning Notice	This Warning Notice is mandatory: OFFICIAL: Sensitive RSEN WARNING: Risk Sensitive (RSEN) information is derived from sensitive imaging operations. This handling instruction is designed to protect and emphasise the sensitivity of certain imaging operations, as well as the products and intelligence associated with those capabilities. Contact the Controlling Authority (AGO) for Further Information.
Sanitisation	Contact the Controlling Authority (AGO) for approval.
Referencing	Refer to Referencing Intelligence.
Destruction	**Electronic**: See the *Information security manual* for further details. **Physical**: According to the PSPF instructions for the security classification of the material.
Further Information	Contact the Controlling Authority (AGO)—see Security Caveat Controlling Authorities.

8.5. STRAP (United Kingdom—UK)

Refer to the classified annex of this Standard for Further Information.

Controlling Authority	Australian Secret Intelligence Service (ASIS) by proxy for UK HUMINT Australian Signals Directorate (ASD) by proxy for UK SIGINT
Access Requirements	Minimum prerequisite Negative Vetting 2 (NV2)
Briefing Requirements	CHARLIE briefing for UK HUMINT DELTA briefing for UK SIGINT
Security Classifications	SECRET/TOP SECRET **Whatever its classification, STRAP material must be stored, processed and transmitted only on TOP SECRET systems.**
Definition	The STRAP caveat denotes UK material that is sensitive or requires restricted handling. STRAP reporting may contain UK HUMINT and/or UK SIGINT material.
Application	Refer to the classified annex of this Standard for Further Information.
Handling Requirements	**Must be treated as accountable material.** Refer to the classified annex of this Standard for Further Information.
Warning Notice	Refer to the classified annex of this Standard for Further Information.
Sanitisation	As per COMINT
Referencing	Refer to Referencing Intelligence.
Destruction	As per COMINT
Further Information	Contact the Controlling Authority (ASIS or ASD as appropriate)—see Security Caveat Controlling Authorities.

8.6. Other Foreign Government Markings (Non-Caveat)

The following Foreign Government Markings (FGMs) are not caveats as they are not applied to security classified information.

While the information does not require a classification, Australian entities apply these FGMs to material to maintain protection for the same purposes as other FGMs.

8.6.1. CUI—Controlled Unclassified Information (United States)

Controlling Authority	National Intelligence Community
Access Requirements	No specific security clearance or access is required to read CUI information.
Briefing Requirements	Nil
Security Classifications	N/A
Definition	This is a United States marking that is being implemented progressively and is expected to replace UNCLASSIFIED and FOUO. This marking is defined within the National Institute of Standards and Technology, USA, *Recommended security controls for federal information systems and organizations*, August 2009: A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the federal government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. Henceforth, the designation CUI replaces Sensitive But Unclassified (SBU). **Note**: the US caveat limited distribution (LIMDIS) is a subset of CUI.
Application	**Handle as OFFICIAL: Sensitive.**
Handling Requirements	As per OFFICIAL: Sensitive
Warning Notice	N/A
Sanitisation	Refer to the originator.
Referencing	Refer to Referencing Intelligence.
Destruction	**Electronic**: See the *Information security manual* for further details. **Physical**: According to the PSPF instructions for the security classification of the material.
Further Information	N/A

8.6.2. LIMDIS—Limited Distribution (United States)

Controlling Authority	Australian Geospatial-Intelligence Organisation (AGO) by proxy
Access Requirements	All Defence and Australian Intelligence Community (AIC) personnel may see or receive limited distribution (LIMDIS) material at any time for official use. For any further release of LIMDIS product, apply in writing to AGO Customer Services.
Briefing Requirements	N/A
Security Classification	OFFICIAL
Definition	LIMDIS is a caveat used by United States National Geospatial-Intelligence Agency to protect OFFICIAL maps and other controlled OFFICIAL geospatial products. LIMDIS is a subset of CUI—Controlled Unclassified Information (United States).
Application	Australian agencies may not apply this US caveat other than to carry it forward from existing caveated material. If an Australian agency is seeking a security caveat to limit access to information to a list of named recipients, the EXCLUSIVE FOR caveat should be used. Header/footer examples: OFFICIAL LIMITED DISTRIBUTION OFFICIAL//LIMITED DISTRIBUTION OFFICIAL//LIMDIS **If the classification of the material is PROTECTED or higher, the LIMDIS marking is not used.**
Handling Requirements	**Electronic handling**: LIMDIS material can be stored on a classified or OFFICIAL system, or in hard copy, such that it is accessible by Defence and AIC personnel only and other approved LIMDIS users. Unless systems have been safeguarded using Defence-approved authentication and encryption technology, LIMDIS data cannot be: used or stored on publicly accessible systems, such as the internet or other systems accessible by unauthorised individuals; or sent over unclassified computers or networks such as the internet or on other systems accessible by unauthorised individuals. **Physical handling**: As per OFFICIAL. **Storage**: As per OFFICIAL.
Warning Notice	This Warning Notice is mandatory: Distribution authorised to DoD, IAW 10 U.S.C §§ 130 & 455. Release authorized to U.S. DoD contractors, IAW 48 C.F.R § 252.245-7000. Refer other requests to: Headquarters NGA, ATTN: Release Officer, Mail Stop S82-OIAD, 7500 Geoint Drive, Springfield, VA 22150-7500. Destroy IAW DoDD 5030.59. Removal of this caveat is prohibited.
Sanitisation	The LIMDIS status of products produced derived from a LIMDIS source is usually transferred to the new product. Applications to remove the caveat, which are assessed on a case-by-case basis, must be made in writing to AGO Customer Services.
Referencing	Refer to Referencing Intelligence. **Caution**: When referencing information that has been marked with a releasability caveat, the new material must not be distributed more widely than the original. Contact the Controlling Authority (AGO) for advice.
Destruction	**Electronic**: See the *Information security manual* for further details. **Physical**: According to the PSPF instructions for the security classification of the material.
Further Information	Contact the Controlling Authority (AGO)—see Security Caveat Controlling Authorities.

9. Special Handling Instructions

Special handling instructions on material indicate specific precautions that must be taken.

9.1. DELICATE SOURCE

Controlling Authority	Australian Secret Intelligence Service (ASIS)
Access Requirements	A Positive Vetting (PV) or TOP SECRET-Privileged Access (TS-PA) security clearance is required for regular, ongoing access to, or for the generation of, DELICATE SOURCE material. In limited circumstances a Negative Vetting 2 (NV2) security clearance may suffice for irregular and/or a finite period of access, subject to approval from ASIS.
Briefing Requirements	CHARLIE briefing, administered by ASIS or delegated agency Special Security Officer (SSO)
Security Classifications	SECRET/TOP SECRET **Whatever its classification, DELICATE SOURCE material must be stored, processed and transmitted only on TOP SECRET systems.**
Definition	DELICATE SOURCE is used in Australia to handle and distribute HUMINT information that is sensitive or requires restricted handling.
Application	Header/footer examples: TOP SECRET DELICATE SOURCE TOP SECRET//DELICATE SOURCE **ORCON caveat**: DELICATE SOURCE material does not require the ORCON caveat to also be applied. However, ORCON may be present for other reasons—for example, to ensure correct handling by Five-Eyes countries. See Section 9.2. **Five-Eyes distribution**: When passing DELICATE SOURCE material to Five-Eyes countries, the DELICATE SOURCE caveat must be replaced by the ORCON caveat. The material must still be stored, processed and transmitted on TOP SECRET systems only.
Handling Requirements	**Must be treated as accountable material.** **Electronic handling**: Material must be stored, processed and transmitted electronically on a TOP SECRET–accredited sensitive compartmented information (SCI) system. **Physical handling**: In addition to the handling instructions for the respective classification (SECRET or TOP SECRET), material should be passed to confirmed CHARLIE-briefed people only. **Storage**: Material must be stored and processed within a Security Zone 5 (as defined in the PSPF) unless otherwise advised. Consult ASIS for further details. **Legal**: ASIS-generated material is exempt from certain federal Acts (e.g. the *Privacy Act*) and certain sections of other federal Acts (e.g. the Archives and FOI Acts). DELICATE SOURCE material may not be published by a receiving agency beyond the original distribution of the material without the prior approval of ASIS. An agency may develop an agreement with ASIS regarding the further distribution or use of its DELICATE SOURCE material. Contact ASIS for information about these agreements.
Warning Notice	A Warning Notice may be required, subject to agreement with ASIS.
Sanitisation	For all requests, contact the Controlling Authority (ASIS) for approval. Refer to the classified annex of this Standard for Further Information.
Referencing	Refer to Referencing Intelligence.
Destruction	**Electronic**: See the *Information security manual* for further details. **Physical**: According to the PSPF instructions for the security classification of the material.
Further Information	Contact the Controlling Authority (ASIS)—see Security Caveat Controlling Authorities.

9.2. ORCON—originator controlled

Controlling Authority	Australian Security Intelligence Organisation (ASIO) Australian Secret Intelligence Service (ASIS) Australian Geospatial-Intelligence Organisation (AGO) Australian Signals Directorate (ASD) Defence Intelligence Organisation (DIO) Office of National Intelligence (ONI)
Access Requirements	There are no security clearance or briefing requirements for ORCON material.
Briefing Requirements	N/A
Security Classifications	PROTECTED and above
Definition	The ORCON caveat can only be applied by listed Controlling Authority agencies. ORCON material may be accessed within the receiving agency but may not be distributed beyond that agency without the prior approval of the originating Controlling Authority agency. The receiving agency must seek approval from the originator Controlling Authority agency before the applying the ORCON caveat to their own reporting information or referencing ORCON derivative information in their own reporting materials.
Application	Header/footer examples: SECRET ORCON SECRET//ORCON An ORCON Warning Notice must also be displayed.
Handling Requirements	**ORCON material may be transmitted on any classified system—that is, it is not restricted to a TOP SECRET system.** ORCON material must not be repurposed, distributed or published by a receiving agency beyond the original distribution of the material without the prior approval of the originating agency. An agency may develop an agreement with the originating agency to further distribution or use of its ORCON material. See section 15.1 of this Standard. **Caution**: Not all other countries have an equivalent caveat to ORCON and may therefore interpret this caveat differently.
Warning Notice	Originating agencies must apply an appropriate Warning Notice directing recipients how to handle ORCON material.
Sanitisation	Contact the Controlling Authority for approval.
Referencing	Refer to Referencing Intelligence.
Destruction	**Electronic**: See the *Information security manual* for further details. **Physical**: According to the PSPF instructions for the security classification of the material.
Further Information	Contact the Controlling Authority (ASIO, ASIS, AGO, ASD, DIO or ONI as appropriate)—see Security Caveat Controlling Authorities.

9.3. EXCLUSIVE FOR

Controlling Authority	Originator
Access Requirements	There are no security clearance or briefing requirements for EXCLUSIVE FOR material.
Briefing Requirements	N/A
Security Classifications	PROTECTED and above
Definition	This is a special-handling caveat that indicates the information must be accessed only by the named recipients. A recipient can be a named person, a position title or a designation.
Application	Header/footer examples: EXCLUSIVE FOR
Handling Requirements	If the recipient is not available to action/open the material, the receiving agency must contact the originating agency and seek approval for an alternative recipient of the material. EXCLUSIVE FOR replaces the legacy marking ADDRESSEE ONLY. EXCLUSIVE FOR must not be confused with or applied instead of LIMDIS, a foreign government marking (US).
Warning Notice	This Warning Notice is optional: If the recipient is not available to action/open the material, the receiving agency must contact the originating agency and seek approval for an alternative recipient.
Sanitisation	Contact the Controlling Authority for approval.
Referencing	Refer to Referencing Intelligence.
Destruction	**Electronic**: See the *Information security manual* for further details. **Physical**: According to the PSPF instructions for the security classification of the material.
Further Information	Contact the Controlling Authority—see Security Caveat Controlling Authorities.

9.4. CABINET

Controlling Authority	Department of the Prime Minister and Cabinet (PM&C)
Access Requirements	Minimum prerequisite: Baseline security clearance Strict need-to-know
Briefing Requirements	N/A
Security Classifications	PROTECTED and above
Definition	Cabinet documents are defined in the Cabinet Handbook and the *Freedom of Information Act 1982* (FOI Act). They include material that: • is prepared to inform the Cabinet (e.g. submissions, memoranda or papers and their attachments or supporting documents; coordination comments; and any other documents which are both identical in all relevant respects to those considered by the Cabinet and precursors of documents submitted to the Cabinet); • reveals the decision and/or deliberations of the Cabinet (including business lists, Cabinet minutes, notes taken by Cabinet note takers, and Cabinet meeting dates); • is prepared by departments to brief their ministers on matters proposed for Cabinet consideration; and • has been created to inform a proposal to be considered by the Cabinet (such as drafting comments or departmental cost analysis).
Application	Header/footer examples: PROTECTED CABINET PROTECTED//CABINET
Handling Requirements	**Must be treated as accountable material.** Entities are required to maintain a record of who has had access to each Cabinet document. **Electronic handling**: Whatever its classification, documents in a Cabinet template must be stored, processed and transmitted between entities on Cabinet Division-approved systems only (e.g. CabNet+). Other supporting documentation must be transmitted on appropriately classified networks and only between officers with a clear need-to-know. **Physical handling**: As per classification. Additionally: **Copies**: Cabinet documents in the Cabinet template must not be copied. This rule includes transcribing or copying of text of Cabinet documents into departmental ICT systems. The production and circulation of Cabinet minutes is strictly controlled by the Cabinet Division. If copies of these are required, submit a request to the Cabinet Division including information on why access is being sought. **Physical storage:** CABINET documents must be kept in Cabinet-specific files that are appropriately classified. CABINET documents must be stored in secure containers appropriate to their classification. **Legal**: The FOI Act recognises the special nature of Cabinet deliberations in the exemption it provides for certain Cabinet documents from disclosure. Requests to access Cabinet documents and Cabinet-related material under the FOI Act must be handled in consultation with PM&C's Freedom of Information Coordinator.
Warning Notice	N/A
Sanitisation	Obtain approval from the Controlling Authority
Referencing	**Electronic**: See the *Information security manual* for further details. **Physical**: Either according to the PSPF instructions for the classification level; or returned to the Cabinet Division.
Destruction	Refer to the Cabinet Handbook or consult the Cabinet Division of the Department of the Prime Minister and Cabinet (PM&C)
Further Information	Minimum prerequisite: Baseline security clearance Strict need-to-know Contact the Controlling Authority (PM&C)—see Security Caveat Controlling Authorities.

10. Releasability Caveats

Releasability caveats limit access to information based on citizenship.

No more than one releasability caveat may be applied in a protective marking.

Caution: the absence of a releasability caveat defaults the material to a different releasability in different agencies. For example:

- The Department of Defence and Defence agencies treat information with no releasability caveat as equivalent to REL AUS/CAN/GBR/NZL/USA.
- Other Australian Government agencies treat information with no releasability caveat as AUSTEO.

When referencing information that has been marked with a releasability caveat, the new material must not be distributed more widely than the original.

10.1. National Intelligence Community

The National Intelligence Community comprises:

- Office of National Intelligence (ONI)
- Australian Signals Directorate (ASD)
- Australian Geospatial-Intelligence Organisation (AGO)
- Australian Secret Intelligence Service (ASIS)
- Australian Security Intelligence Organisation (ASIO)
- Defence Intelligence Organisation (DIO)
- Australian Criminal Intelligence Commission (ACIC), and
- the intelligence functions of the:
    - Australian Federal Police (AFP),
    - Australian Transaction Reports and Analysis Centre (AUSTRAC), and
    - Department of Home Affairs.

10.2. AGAO—Australian Government Access Only

Controlling Authority	Originator
Access Requirements	Appropriately cleared Australian citizens, and appropriately cleared representatives of Five-Eyes foreign governments on exchange or long-term posting or attachment in the National Intelligence Community and the Department of Defence. Agencies other than members of the National Intelligence Community (ONI, ASD, AGO, ASIO, ASIS, ACIC, AFP, AUSTRAC, DIO and Home Affairs), Defence and the Australian Submarine Agency must treat AGAO material as if it were marked AUSTEO.
Briefing Requirements	N/A
Security Classifications	PROTECTED and above AGAO material must be stored, processed and transmitted on systems that enforce citizenship-based access controls.
Definition	AGAO denotes Australian Government information that may be accessed by appropriately cleared representatives of Five-Eyes foreign governments on exchange or long-term posting or attachment in the National Intelligence Community, Defence and the Australian Submarine Agency. This access is granted on the proviso that AGAO information must not be distributed to the representative's parent agency/s or respective country/s or outside Australia. AGAO must not be used in conjunction with the AUSTEO or REL releasability caveats.
Application	Header/footer examples: SECRET AGAO SECRET//AGAO
Handling Requirements	Agencies other than members of the National Intelligence Community (ONI, ASD, AGO, ASIO, ASIS, ACIC, AFP, AUSTRAC, DIO and Home Affairs), Defence and the Australian Submarine Agency must treat AGAO material as if it were marked AUSTEO. **Electronic handling**: Where non-Australian citizens are users or administrators, agencies must prevent the inadvertent or deliberate unauthorised access to AGAO material. See the *Information security manual* for Further Information. AGAO material must be stored, processed and transmitted on systems that enforce AGAO access controls—that is, SECRET and above. **Physical handling**: As per security classification **Physical storage**: Must be segregated to ensure non-Australian citizens do not have access.
Warning Notice	This Warning Notice is recommended but optional: This is Australian Government Access Only (AGAO) material. AGAO material is releasable to Australian nationals only and to appropriately cleared and briefed representatives of the United States, United Kingdom, Canada and New Zealand who have a strict need-to-know and are integrated in or working on behalf of the National Intelligence Community and the Department of Defence. Agencies other than members of the National Intelligence Community (ONI, ASD, AGO, ASIO, ASIS, ACIC, AFP, AUSTRAC, DIO and Home Affairs), Defence and the Australian Submarine Agency must treat AGAO material as if it were marked AUSTEO. AGAO material may be incorporated only in assessments and material marked AGAO or AUSTEO.
Sanitisation	Contact the Controlling Authority for approval.
Referencing	Refer to Referencing Intelligence. AGAO material may be referenced only in material marked AGAO or AUSTEO. **Caution**: When referencing AGAO material, the new material must not be distributed more widely than the original. Contact the Controlling Authority for advice.
Destruction	**Electronic**: See the *Information security manual* for further details. **Physical**: According to the PSPF instructions for the security classification of the material.
Further Information	Contact the Controlling Authority— see Security Caveat Controlling Authorities.

10.3. AUSTEO—Australian Eyes Only

Controlling Authority	Originator
Access Requirements	Strictly Australian citizens only (unless an exemption is granted). Holding of additional citizenship does not preclude access.
Briefing Requirements	N/A
Security Classifications	PROTECTED and above **AUSTEO material must be stored, processed and transmitted on systems that enforce citizenship-based access controls.**
Definition	AUSTEO denotes Australian Government information that must be restricted to Australian citizens exclusively. No policy exception may be made to the requirement for Australian citizenship for AUSTEO access unless an exemption is granted after meeting specific requirements. See PSPF Requirement 0080 for the exemption process and requirements. AUSTEO must not be used in conjunction with the AGAO or REL releasability caveats.
Application	Header/footer examples: SECRET AUSTEO SECRET//AUSTEO
Handling Requirements	**Electronic handling**: Where non-Australian citizens are users or administrators, agencies must take appropriate steps to prevent the inadvertent or deliberate unauthorised access to AUSTEO material. Refer to the *Information security manual* for Further Information. **AUSTEO material must be stored, processed and transmitted only on systems that enforce AUSTEO controls—that is, SECRET and above.** **Physical handling**: As per security classification **Physical storage**: Must be segregated to ensure non-Australian citizens do not have access.
Warning Notice	This Warning Notice is recommended but optional: This is Australian Eyes Only (AUSTEO) material. It is releasable to Australian nationals only. AUSTEO material may be incorporated only in assessments and material marked AUSTEO.
Sanitisation	Only the originating agency can reconsider application of the AUSTEO caveat and where appropriate, sanitise AUSTEO material to allow releasability to non-Australian citizens. The sanitised information cannot be released to non-Australian citizens without agreement from the originating agency.
Referencing	Refer to Referencing Intelligence. AUSTEO material must only be referenced in material marked AUSTEO. **Caution**: When referencing information that has been marked with a releasability caveat, the new material must not be distributed more widely than the original. Contact the Controlling Authority for advice.
Destruction	**Electronic**: See the *Information security manual* for further details. **Physical**: According to the PSPF instructions for the security classification of the material
Further Information	Contact the Controlling Authority— see Security Caveat Controlling Authorities.

10.4. REL—Releasable To

Controlling Authority	Originator
Access Requirements	Citizenship of at least one country listed in the REL marking The REL caveat is an exclusive marking in that it disqualifies a third-party national seconded or embedded within a foreign government agency from accessing the information. For example, material marked REL AUS/GBR must be accessible by Australian and United Kingdom citizens only and must not be accessible by a person of another nationality, regardless of whether that person is working in or otherwise attached to the Australian Government.
Briefing Requirements	N/A
Security Classifications	PROTECTED, SECRET, TOP SECRET
Definition	The REL caveat identifies information that: • an originator has predetermined is releasable or has been released through established foreign disclosure memorandums of understanding, procedures and channels; and • may be accessed by a national of one of the countries listed in the REL marking who meets the criteria of all other protective markings; has a need to know; and is employed in an agency of their country or represents their country in a relevant Australian Government or international agency. **Caution**: The absence of a releasability caveat will result in the information being treated differently by different agencies.
Application	The following guidelines apply when using the REL protective marking: • REL uses all capital letters, followed by a single space character, then two or more country codes in alphabetical order that are separated by a single forward slash (/) character. • Country codes are the standard trigraphs defined in ISO 3166-1:2013. • REL must not be used in conjunction with any other releasability caveat. • FVEY is not an Australian marking and must not be used. Header/footer examples: TOP SECRET COMINT REL AUS/CAN/GBR/NZL/USA TOP SECRET//COMINT/REL AUS/CAN/GBR/NZL/USA
Handling Requirements	**Electronic handling**: Must be handled on systems that can enforce releasability controls. See the *Information security manual* for Further Information. **Physical handling**: As per security classification **Storage**: In addition to the storage requirements of all other protective markings, REL material must be segregated where a releasability caveat excludes a person who would have otherwise had access.
Warning Notice	N/A
Sanitisation	Contact the Controlling Authority for advice.
Referencing	Refer to Referencing Intelligence. **Caution**: When referencing information that has been marked with a releasability caveat, the new material must not be distributed more widely than the original. Contact the Controlling Authority for advice.
Destruction	**Electronic**: See the *Information security manual* for further details. **Physical**: According to the PSPF instructions for the security classification of the material.
Further Information	Contact the Controlling Authority— see Security Caveat Controlling Authorities.

11. Accountable Material

The requirements for handling and storing accountable material are outlined in PSPF Release 2025– Classifications and Caveats.

12. Handling, Transport and Storate Requirements

All people who handle security-caveated material—physical or electronic—must be aware of the caveat's handling, transport and storage requirements, in addition to applying the need-to-know principle.

The requirements for handling, storing and transporting classified material are outlined in the PSPF Release 2025.

12.1. Courier Services

The special Handling Requirements for certain caveats may preclude the use of an endorsed courier service.

- For information on courier services for classified material within Australia, contact ASIO's T4 directorate via t4ps@t4.gov.au (unclassified) or 02 6234 1217.
- For information on the overseas carriage of classified material, contact the Department of Foreign Affairs and Trade.

13. Derivative Material

Derivative material draws on, summarises or quotes one or more sources of intelligence. Summaries, assessments and briefings are common forms of derivative material.

The protective markings on the derivative material must not be lower than the source material.

If the derivative material has the same or more restrictive protective markings and will not be distributed any further than the source material, the originator's approval is usually not required. Handling notices in the source material will indicate whether the originator's approval is required.

Derivative material must display the Warning Notice for each of its caveats.

14. Referencing Intelligence

Referencing intelligence is the identification of intelligence that has been published by one agency within material published by another.

14.1. Referencing by Title

Generally, the title of a security-classified report carries the same classification as the report to which it belongs.

A referencing report should only reference the title of an original report if the referencing report's classification and protective markings are the same as or more restrictive than the original report's and if the readership for both reports is similar—for example, both reports have been released on a SECRET system.

Originating agencies may reduce the classification of the title of their own report, taking into consideration the points mentioned above. If there is doubt over the classification of a title, contact the originator of the report.

14.2. Referencing by Number Only

Citation of intelligence material by its identification number—for example, report number ABC 123/2018—without reference to its title, its content or the originating entity, is usually OFFICIAL.

ASD prefers its COMINT reports to be referenced by number only.

14.3. Referencing by Entity

Material that attributes intelligence to a particular entity—with or without the identification number or title—must carry the same protective markings (including security caveats) as the original material, or higher protective markings, unless the originator's approval for different protective markings has been received.

The exception to this rule is when a reference does not indicate any sensitive information.

- For example, if an entity's report titled Daily summary is not marked with a codeword and references another of the same entity's report titled Daily summary that is marked with a codeword, the reference is permitted if the generic title and context of the reference do not reveal any sensitive information.

Material that attributes ASIS intelligence in a report classified SECRET should be 'according to secret reporting' and must not reference ASIS.

Reporting from foreign agencies must be referenced to comply with foreign security requirements—seek advice from the security or intelligence publishing area of your entity.

14.4. Referencing Without Attribution

Derivative material must have the same protective markings as, or higher protective markings than, the source material, or the relevant portion where portion markings are used, unless approval is received from the originating entity.

15. Further Distribution of Intelligence

15.1. By Agreement

Agencies may make agreements that allow one agency to further distribute the published intelligence material of another. These agreements should be in writing and registered by both agencies. These agreements do not extend to embedded liaison personnel from a third agency.

15.2. Sanitisation

Intelligence may require sanitisation (modification) to maximise its potential and securely broaden its distribution. Sanitisation is the process of editing, disguising or otherwise altering intelligence material to permit distribution with less restrictive protective markings to a wider audience while maintaining protection of sensitive sources, methods, capabilities, analytical procedures and privileged information.

The originator is responsible for controlling its material's sanitisation. An agency must obtain the originator's approval to sanitise material.

Entities may make agreements that allow one entity to sanitise the published intelligence material of another. These agreements should be in writing and registered by both entities.

An originator may provide a pre-approved form of sanitisation, known as a tearline, in a document.

15.2.1. Tearline

Within a classified document, a tearline is a clearly marked portion, approved by the originator, containing sanitised information with less-restrictive protective markings than the document in which it is contained.

A tearline may include handling instructions.

When an entity uses or distributes material contained in a tearline, they must ensure that the material is not associated in any way with the original report, originating entity, or type of intelligence collection.

The following is an example of a tearline classified PROTECTED.

PROTECTED

TEARLINE BEGINS

Tearline content goes here.

TEARLINE ENDS

PROTECTED

---

16. Classified Annex

Refer to the separate Classified Annex of this Standard (available on Pensieve) for Further Information.

17. Historical Security Caveat Register

There are historical security caveats that have been retired and ceased from use, as they no longer reflect Australian Government policy. The mandatory elements for handling security caveated information and accountable material remain for material marked with historical security caveats.

Historical security caveats cannot be applied to material created after the date the security caveat use was ceased.

The controlling authority retains responsibility for managing and administering historical security caveats. Refer to Controlling Authorities for details.

17.1. NATIONAL CABINET (Historical)

Controlling authority	Department of the Prime Minister and Cabinet (PM&C)
Status	Ceased on 21 March 2025
Category	Special Handling Instructions
Access requirements	Minimum prerequisite: Baseline security clearance when applied with PROTECTED. No security clearance requirements when applied with OFFICIAL: Sensitive. Strict need-to-know
Briefing requirements	N/A
Security classifications	OFFICIAL: Sensitive and above
Definition	National Cabinet documents includes material that: a) is prepared for the purpose of informing the National Cabinet and/or its subcommittees (e.g. submissions, papers and their attachments or supporting documents, and any other documents which are both identical in all relevant aspects to those considered by National Cabinet and precursors of documents submitted to the National Cabinet)

Controlling authority	Department of the Prime Minister and Cabinet (PM&C)
	b) reveal the decision and/or deliberations of the National Cabinet and/or its subcommittees (including business lists, minutes, notes taken by Commonwealth and State/Territory note-takers, and meeting dates), or c) is prepared by Commonwealth or State and Territory departments to brief the Prime Minister, First Ministers and Commonwealth and State and Territory members of the National Cabinet subcommittees on matters proposed for National Cabinet consideration.
Application	Header/footer examples: PROTECTED NATIONAL CABINET PROTECTED//NATIONAL CABINET OFFICIAL: Sensitive NATIONAL CABINET OFFICIAL: Sensitive//NATIONAL CABINET
Handling requirements	**Must be treated as accountable material.** Entities are required to maintain a record of who has had access to each National Cabinet document. • **Electronic handling**: National Cabinet documents must be transmitted on appropriately sensitive or classified networks and only between officers with a clear need-to-know. Where possible, documents in a National Cabinet template must be stored, processed and transmitted between entities on Cabinet-Division approved systems and/or State and Territory Cabinet systems. • **Physical handling**: As per classification. Additionally: – **Physical storage:** National Cabinet documents must be kept in National Cabinet-specific files that are appropriately classified. National Cabinet documents must be stored in secure containers appropriate to their protective marking or classification. • **Legal**: The FOI Act and judicial or inquisitorial processes recognise the special basis for preserving confidentiality of Cabinet deliberations in exemptions and immunities from disclosure applied to Cabinet documents and information. National Cabinet has been constituted as a Cabinet Committee. Requests to access National Cabinet documents (as defined above) under the FOI Act must be handled in consultation with PM&C's Freedom of Information Coordinator, as set out in the Cabinet Handbook, and other requests for access must be handled in consultation with the Cabinet Division of PM&C.
Warning notice	N/A
Sanitisation	Obtain approval from the controlling authority
Referencing	• **Electronic**: See the *Information security manual* for further details. • **Physical**: Either according to the PSPF instructions for the protective marking or classification level; or returned to the Cabinet Division.
Destruction	Refer to the Cabinet Handbook or consult the Cabinet Division of the Department of the Prime Minister and Cabinet (PM&C)
Further information	Minimum prerequisite: Baseline security clearance when applied with PROTECTED. No security clearance requirements when applied with OFFICIAL: Sensitive. Strict need-to-know

ANNEX A

Request Form: New Security Caveat/National Compartment – and/or – Amend Existing Security Caveat/National Compartment

Please complete and submit to PSPF@homeaffairs.gov.au.

Part 1: Request Type and Business Case

Entity Name	
Entity Contact	
Request Type	☐ New Security Caveat
	☐ Amendment to existing Security Caveat
	☐ New National Compartment
	☐ Amendment to existing National Compartment
Business Case	

Part 2: Security Caveats

Amendment to Security Caveat	
Name of Caveat	Name of existing caveat
Amendments	Proposed amendments
New Security Caveat	
Security Caveat Category	Codewords, Foreign Government Markings, Special Handling Instructions, or Releasability Caveats
Caveat Name	Proposed name and any permitted short-form
Controlling Authority	
Contact Details	
Access Requirements	Minimum prerequisite security clearance and need-to-know requirements for access, including where use is restricted to specific entities (list the entities and reason for the restricted use)
Briefing Requirements	Compartmental or other briefings
Security Classification	OFFICIAL: Sensitive, PROTECTED, SECRET or TOP SECRET
Definition	If the details of the caveat's application are classified, refer users to the Classified Annex of the Security Caveat Standard
Application	Guidelines for use and Header/Footer examples
Handling Requirements	Electronic and physical Handling Requirements, storage and any legal requirements
Warning Notice	If required
Sanitisation	Contact details to request changes
Referencing	Identify intelligence that has been published by one agency within material published by another

Destruction	Electronic and physical destruction requirements (reference PSPF and/or ISM)
Further Information	Contact details for the Controlling Authority.

Part 3: National Compartments

Amendment to National Compartment	
Name of National Compartment	
Amendments	
New National Compartment	
Compartment Name	Name assigned by billet system
Associated Security Caveat	The associated security caveat/codeword
Controlling Authority	
Contact Details	
Access Requirements	Minimum prerequisite security clearance and need-to-know requirements for access, including where use is restricted to specific entities (list the entities and reason for the restricted use)
Briefing Requirements	Details of any specific indoctrination requirements that must be met in order to have access to information within the Compartment.
Compartment Briefing Officer	Name of the Compartment Briefing Officer role authorised to brief authorised personnel into this compartment
Security classifications	OFFICIAL: Sensitive, PROTECTED, SECRET or TOP SECRE
Further Information	Contact details for the Controlling Authority.