GUIDANCE – CLASSIFYING AND DISTRIBUTING OFFICE INFORMATION

ENDORSED SEPTEMBER 2025

About this document	
Purpose	This Guidance document provides instructions on how to classify information in the Office of the Commonwealth Ombudsman (the Office), based on the Australian Government Protective Security Policy Framework (PSPF) and Information Security Manual (ISM). This Guidance document replaces two documents previously released via the Office intranet and which were titled *Classifying information procedure* (identified as A2404564) and *Guide to assessing and protecting Official information* (identified as A2412248).
User/s	All Office staff, including contractors and consultants.
Publication/release to other sites	This Guidance document is being released to the VOLT platform, which is internal to the Office. It has not been published on an external website and is not intended for external publication.
Outcome	Staff understand the role and importance of information security and the correct classification of information Staff classify information correctly Staff share and exchange information externally according to its classification
Version number	1.1
Consultation	Legal team, DIAL Branch Security team, Corporate Branch
Approved/endorsed by	Chief Information Officer, Corporate Branch
Date approved/endorsed	September 2025 (Version 1.0) January 2026 (Version 1.1)
Next review date	September 2026 post annual PSPF update
Contact team	ICT, Security and Information Management Team, Corporate Branch

Contents

References and documents 2
Overview of Classifying Information in the Australian Government 3
How to Classify, Protect and Transmit Official Information 5
Recording Official Information 6
Reporting Suspected Data/Information Breaches 6
Appendix A: Quick Guide to Classifying Information in the Office 7
Appendix B: Information Classification Usage Tables 8
Appendix C: Privacy Act 1998 definition of personal information 16

References and documents

- Australian Government Protective Security Policy Framework (PSPF Release 2025)
- Australian Government Information Security Manual (ISM)
- PM&C Cabinet Handbook
- ICT Acceptable Use Policy 2024
- ICT Security Policy 2024
- Security Classifications, IT Hub and Information Management | IT Hub
- Information Management Strategy 2025–28
- Guidance – Information Management within the Office of the Commonwealth Ombudsman: Systems of Record
- Guidance – Use of Fortress for PROTECTED information
- Commonwealth Ombudsman Privacy Policy

Overview of Classifying Information in the Australian Government

The Office classifies information according to the Protective Security Policy Framework (PSPF). The PSPF assists Australian Government entities to protect their people, information and assets, both at home and overseas, by setting out government protective security policy for security governance, information security, personnel security and physical security.

As the PSPF outlines, information can be collected, used, stored and transmitted in many forms, including electronically, physically and audibly.

Basic Concepts in Information Classification and Handling:

- **Need-to-Know Principle:** Reflects the need for personnel to only access information where there is a requirement to do so to fulfil their official duties, and applies to all official and security-classified information.
- **Classification:** The assessed rating that is given to all information that is created within the Australian Government and reflects the level of harm and damage that could occur to individuals, organisations and government if compromised. OFFICIAL and UNOFFICIAL are **not security classifications.**
- **Security Classification:** The level of security classification determines the level of physical and electronic protections and handling requirements for that information. The Australian Government uses four security classifications:
    - OFFICIAL: Sensitive
    - PROTECTED
    - SECRET
    - TOP SECRET
- **'Official' Information:** Official information is the collective term for all information created, sent or received as part of the work of the Australian Government, except for information that is classified UNOFFICIAL.
- **Information Management Markers (IMMs)**: IMMs are an optional way to add additional access and use restrictions to security-classified information. The IMMs currently available to be used with security-classified information are:
    - Personal Privacy (see **Appendix C** for definition of personal information)
    - Legal Privilege
    - Legislative Secrecy

  Note: Only one IMM can be applied to a document or correspondence in the Office Network. If multiple IMMs are applicable for the topic, selected in the following order:

  1. Legislative Secrecy
  2. Legal Privilege
  3. Personal Privacy

- **Security Caveat:** Security Caveats are a warning that the information has special protections in addition to those indicated by the security classification. Security Caveats are not classifications and must appear with a security classification. **For the Office, Security Caveats only apply for security classifications PROTECTED and above.**

- **Protective Marking:** Protective Markings are text-based markings that appear on documents to indicate the security classification, Security Caveats (if applicable) and IMMs (if applicable). It is mandatory for all security-classified information and optional for OFFICIAL.

- **Security Clearance:** A security clearance is a statement of assurance that a person is both eligible and, so far as can be determined at the time that the clearance is issued, suitable to hold a position of trust that gives them access to security-classified Australian Government information, resources and activities.

  Security vetting is conducted to determine whether an individual is eligible and suitable to hold a security clearance in order to access security-classified government information, resources and activities. To be eligible for an Australian Government security clearance, an individual must be an Australian citizen, have a checkable background, and possess and demonstrate integrity and trustworthiness commensurate with the security-classified information, resources and activities they will be expected to protect.

This table provides the classification, minimum security clearance requirement and the Office's usage of these classifications:

Classification	Security Classification	Min. Security Clearance	IMMs	Caveats	Office Usage
UNOFFICIAL	NO	Not Required	NO	NO	Office Main Network
OFFICIAL	NO	Not Required	NO	NO	Office Main Network & Fortress
OFFICIAL: Sensitive	YES	Not Required – Police Check	YES	NO	Office Main Network & Fortress
PROTECTED	YES	Baseline	YES	YES	Fortress
SECRET	YES	Negative Vetting Level 1	YES	YES	Paper Files Only (Very Limited)
TOP SECRET	YES	Negative Vetting Level 2	YES	YES	Not available within the Office

How to Classify, Protect and Transmit Official Information

Every staff member who is the originator of information is responsible for selecting the correct classification when sending emails and working with digital documents. When marking information, you are identifying how sensitive or important the information is, who should have access and how the information must be handled.

Appendix A is a **Quick Guide to Classifying Information in the Office**.

Appendix B contains the **Information Classification Usage Tables,** which summarise the common Classifications and IMMs used by the Office, provide examples, and specify the Office's networks that this information can be accessed on, recorded and transmitted through, and who it can be transmitted to.

The incorrect application of classifications can result in information being inappropriately handled, which in turn can result in a reportable security breach.

Changing Classifications: At times it may be necessary to change classifications or add IMMs to information. Office staff are to adopt the following practices when considering changing classifications:

- **Originator is the Office:** the security classification **can be upgraded** to a higher classification **but not downgraded** and an **IMM added but not removed**.
- **Originator is another Australian Government entity**: the security classification and any IMM or caveat **must be retained and not changed**, unless it is suspected to be an error. If an error has been detected, Office staff are to contact the originator to request the information be re-classified and re-transmitted.
- **Originator is an external non-Australian Government entity:**
    - **Where the information already has a classification**, this must be retained and not changed, unless it is suspected to be an error.
    - **For information that doesn't yet have a classification**, Office staff should review the contents and apply an appropriate classification, including any IMM. This is most likely to occur when the information is saved as a record or when responding to an email back to the originator.

Transmitting information: Staff need to ensure that transmission of information is commensurate to the classification and level of protection required for each classification. Staff should adopt the following practices:

- All transmission of information to internal or external recipients must apply the **NEED-TO-KNOW** principle no matter what the classification.
- Transmission of electronic information includes through email, sharing through approved sharing tools, and removable media (e.g. USB Removable Drives).
- **UNOFFICIAL** Information can be transmitted freely to internal and external recipients.

- **OFFICIAL** information can generally be transmitted to internal and external recipients.
- **OFFICIAL: Sensitive including with Information Management Markers** information can generally be **transmitted internally**, *subject to a clear* ***Need-to-Know***. For external recipients, further scrutiny is required:
    - **For external recipients that are other Australian Government entities and personnel prescribed private sector organisations and higher education institutions we oversee,** it is generally acceptable to transmit, *subject to a clear* ***Need-to-Know***.
    - **For all other external recipients,** security-classified information (i.e. OFFICIAL: Sensitive or higher) **should only be disclosed or transmitted** with a person or organisation outside of government to non-Australian Government organisations or individuals **where there is an agreement or arrangement in place**, such as a contract or deed, that establishes handling requirements and protections **UNLESS** the Office is **returning or responding to information provided by a person or organisation outside of government, or their authorised representative**, which the Office subsequently classified as OFFICIAL: Sensitive (*refer to PSPF 2025, Section 12.2.3, Requirement 0077 'Sharing with non-government stakeholders'*).
- **PROTECTED** information (on Fortress) can only be transmitted to recipients that operate on a certified PROTECTED system and to personnel that hold appropriate security clearances.

Recording Official Information

Official information is a record and provides evidence of what an entity has done and why. The Office has four main authorised systems of record to capture official information:

- **For information up to OFFICIAL: Sensitive through the Office's Main Network:**
    - **Resolve** is the Office's case management system
    - **Objective** is the Office's Electronic Document and Records Management System (EDRMS) for saving of business-related records
    - **TechnologyOne (TechOne)** for finance or procurement related documents only.
- **For information up to PROTECTED:** If any part of information being transmitted, stored or saved is at the PROTECTED level, it must occur in Fortress.

For more information on the Office's Systems of Record, refer to Guidance – Information Management within the Office of the Commonwealth Ombudsman: Systems of Record.

Reporting Suspected Data/Information Breaches

If at any time you suspect a data breach or information compromise has occurred, please notify the s 47E(d) [redacted] s 47E(d) [redacted] and s 47E(d) [redacted] during business hours ASAP or out of business hours including weekends call s 47E(d) .

Appendix A: Quick Guide to Classifying Information in the Office

Always follow the ***Need-to-Know* principle** of only accessing and transmitting information where there is a requirement to do so to fulfil official duties.

Classification and IMM	Examples	Distribute To (Transmit To / Share With)
UNOFFICIAL Does not relate to official duties	• A shopping list • Personal reminder • Organising lunch	No restrictions
OFFICIAL Most of our routine information	• General administration and correspondence • Team/branch presentations • Policies, procedures, guidance • Training materials • Publicly released reports • Social Media Content • Position Descriptions/Job Adverts	***Need-to-Know*** principle recommended
OFFICIAL: Sensitive without IMMs Information that requires additional care due to its sensitivity, and could cause limited damage to an individual, organisation or government generally if compromised	• EC, ITGC, ARC papers & minutes • Risk assessments • Branch at a Glance (BaaG) reports • Sensitive case handling • Sensitive investigations • Sensitive internal reports • Senate Estimates briefings • Security Incidents correspondence	***Need-to-Know*** principle applies **Internal recipients**: Office personnel **External recipients**: Australian Government entities and personnel, prescribed private sector organisations and higher education institutions we oversee **Other External recipients**: non-Australian Government organisations or individuals – *ONLY where there is an agreement or arrangement in place*, such as a contract or deed, that establishes handling requirements and protections **UNLESS** the Office is returning or responding to information provided by a person or organisation outside of government, or their authorised representative, which the Office subsequently classified as OFFICIAL: Sensitive
OFFICIAL: Sensitive Personal Privacy IMM OFFICIAL: Sensitive Information that contains personal information in accordance with the Privacy Act	• Documents or correspondence containing personal information about complainants or staff • Conflict of Interest declarations • PDA-related correspondence • Recruitment shortlists & evaluations • WHS Incident Reports	
OFFICIAL: Sensitive Legislative Secrecy IMM	• Draft Bills and draft legislation • Discussion about legislative amendments	
OFFICIAL: Sensitive Legal Privilege IMM	• Requests/instructions for legal advice • Draft or final legal advice • Legal briefings that contain legal advice	***Need-to-Know*** principle applies **All recipients**: Information that is classified OFFICIAL: Sensitive // Legal Privilege **requires the express permission of the Office's Legal Team** before distribution between parties
PROTECTED Information that if compromised could potentially damage the national interest, organisations or individuals	• Commonwealth Budget proposals • Office inspections of law enforcement agencies or places of detention • Analysis of proposed responses to recommendations made in parliamentary committee reports • Cyber Security Post Incident Reports	***Need-to-Know*** principle applies Distributed through Fortress to another certified PROTECTED level system Personnel that hold appropriate security clearances

Appendix B: Information Classification Usage Tables

Appendix B contains 3 usage tables for Office staff summarising how to classify information and provides examples of practical application within the context of the work we do. Appendix B comprises:

- **Table 1** relates to information classified as **UNOFFICIAL** information
- **Table 2** relates to information classified as **OFFICIAL**
- **Table 3** relates to security-classified information: **OFFICIAL: Sensitive** (***including when used with IMMs***) and **PROTECTED**

'Information' refers to information in all formats, digital or non-digital, sent to or received on any Office-issued device, including laptop, mobile phone or tablet. Information means correspondence or documentation. Other digital formats such as Microsoft Teams Chats, multimedia (e.g. photos, videos, audio) that relate to your work for the Office are considered to be of the classification of at least OFFICIAL.

See Guidance – Information Management within the Office of the Commonwealth Ombudsman: Systems of Record for appropriate saving of official information within the Office.

Table 1: Information classified as UNOFFICIAL

Classification	**Examples**	**PERMITTED** / **NOT PERMITTED** — **Use, Store & Transmit ON**		**PERMITTED to Distribute TO (Transmit To / Share With)**
UNOFFICIAL	Information not related to official duties or agency business. Examples: • A shopping list • Personal reminder • Personal Resumes or job applications	**Network:** The Office's Main Network **Record In:** *Not applicable* – UNOFFICIAL information is not to be saved in the Office's Systems of Record	Not applicable	No restrictions

Table 2: Information classified as OFFICIAL				
Classification	**Examples**	**PERMITTED** Use, Store & Transmit ON	**NOT PERMITTED**	**PERMITTED to Distribute TO (Transmit To / Share With)**
OFFICIAL	Most of our routine business, operational and service information is OFFICIAL. Examples: • Administrative records like meeting, minutes, rosters • Operational documents like project plans, service delivery reports, performance metrics • Correspondence like email between staff and or external stakeholders documenting actions, decisions and approvals • Policy and guidance documents like drafts and final versions of policies, procedures and training guides • Financial records like budget spreadsheets, procurement documentation or invoices • HR documentation like job descriptions and recruitment records	**Network:** The Office's Main Network Fortress **Record In:** Resolve Objective TechOne (for finance or procurement documents only) Fortress SharePoint	The Office's Public Websites or Social Media **WITHOUT AUTHORISATION**	Need-to-Know principle recommended **OFFICIAL** marking to be displayed* **Internal recipients**: Office personnel **External recipients**: Australian Government entities and personnel, prescribed private sector organisations and higher education institutions we oversee **External recipients**: non-Australian Government organisations or individuals **The OFFICIAL marking may be omitted for display on the public-release version of an OFFICIAL document*

Security Classified Disclosure and Sharing: Important note: Under PSPF Requirement 0077, the Office has to have an agreement or arrangement, such as a contract or deed, in place that establishes handling requirements and protections before security-classified information or resources are disclosed or shared with a person or organisation outside of government to non-Australian Government organisations or individuals, unless the Office is returning or responding to information provided by a person or organisation outside of government, or their authorised representative, which the Office subsequently classified as OFFICIAL: Sensitive.

For the Office this means, **subject to a clear need to know,** that**:**

- We can provide security-classified information to another Australian Government entity and personnel.
- We can provide security-classified information (OFFICIAL: Sensitive only) to the prescribed private sector organisations and higher education institutions we oversee.
- We can provide security-classified information (OFFICIAL: Sensitive only) to a person or organisation outside of government to non-Australian Government organisations or individuals if we are returning or responding to information provided by a person or organisation outside of government, or their authorised representative, which the Office has subsequently classified as OFFICIAL: Sensitive.
- Under all other circumstances, we need to have a contract or deed in place to ensure the correct handling and protection of security-classified information, e.g. with suppliers and vendors.

Table 3: Security-classified information: OFFICIAL: Sensitive (including when used with IMMs) and PROTECTED				
Classification and Information Management Marker (IMM)	**Examples**	**PERMITTED** / **NOT PERMITTED** **Use, Store and Transmit ON**		**PERMITTED to Distribute TO (Transmit To / Share With)**
OFFICIAL: Sensitive without IMMs **This is a security classification**	Internal reports, complaints, sensitive case handling Information with a contextual sensitivity not linked to a specific legal or privacy obligation. Examples: • Internal risk assessment containing operational vulnerabilities or reputational risk but no personal or legal data • Pre-budget planning documents containing financial sensitivities not linked to IMM-defined sensitivities • Sensitive stakeholder correspondence that may involve contentious negotiations or reputational concerns but not legal privilege or personal privacy	**Network:** The Office's Main Network Fortress **Record In:** Resolve Objective TechOne (for finance or procurement documents only) Fortress SharePoint	The Office's Public Websites or Social Media	Need-to-Know principle applies Display of the **OFFICIAL: Sensitive** marking is mandatory **Internal recipients**: Office personnel **External recipients**: Australian Government entities and personnel, prescribed private sector organisations and higher education institutions we oversee **External recipients**: non-Australian Government organisations or individuals – **ONLY** where there is an agreement or arrangement in place, such as a contract or deed, that establishes handling requirements and protections **UNLESS** the Office is returning or responding to information provided by a person or organisation outside of government, or their authorised representative, which the Office subsequently classified as OFFICIAL: Sensitive

Table 3: Security-classified information: OFFICIAL: Sensitive (including when used with IMMs) and PROTECTED				
Classification and Information Management Marker (IMM)	**Examples**	**PERMITTED** / **NOT PERMITTED** **Use, Store and Transmit ON**		**PERMITTED to Distribute TO (Transmit To / Share With)**
OFFICIAL: Sensitive with Personal Privacy IMM **This is a security classification** Refer to Appendix C for personal information definition	Information containing personal details that require protection under the *Privacy Act 1988* and agency- specific polices. Examples: • Case files involving individuals, such as privacy complaints, referrals, or investigations that include personal data • Recruitment panel assessments including names and contact details • Any documents or correspondence containing personal identifiers. • Medical certificates or leave records that disclose health information or personal circumstances • Internal emails discussing staff issues referencing specific employees	**Network:** The Office's Main Network Fortress **Record In:** Resolve Objective TechOne (for finance or procurement documents only) Fortress SharePoint	The Office's Public Websites or Social Media	Need-to-Know principle applies Display of the **OFFICIAL: Sensitive // Personal Privacy** marking is mandatory **Internal recipients**: Office personnel **External recipients**: Australian Government entities and personnel, prescribed private sector organisations and higher education institutions we oversee **External recipients**: non-Australian Government organisations or individuals – **ONLY** where there is an agreement or arrangement in place, such as a contract or deed, that establishes handling requirements and protections **UNLESS** the Office is returning or responding to information provided by a person or organisation outside of government, or their authorised representative, which the Office subsequently classified as OFFICIAL: Sensitive

Table 3: Security-classified information: OFFICIAL: Sensitive (including when used with IMMs) and PROTECTED				
Classification and Information Management Marker (IMM)	**Examples**	**PERMITTED** / **NOT PERMITTED** **Use, Store and Transmit ON**		**PERMITTED to Distribute TO (Transmit To / Share With)**
OFFICIAL: Sensitive With Legal Privilege IMM **This is a security classification**	Information containing legally privileged content. Examples: • Requests for legal advice • Legal advice, provided internally • Legal advice received from external legal providers • Contains legal interpretations of legislation or contracts • Briefings to senior executives summarising legal risks and options based on advice from internal or external lawyers • Documents containing information about litigation strategy	**Network:** The Office's Main Network Fortress **Record In:** Resolve Objective TechOne (for finance or procurement documents only) Fortress SharePoint	The Office's Public Websites or Social Media	Need-to-Know principle applies Display of the **OFFICIAL: Sensitive // Legal Privilege** marking is mandatory **All recipients**: Information that is classified OFFICIAL: Sensitive // Legal Privilege **requires the express permission of the Office's Legal Team** before distribution between parties

Table 3: Security-classified information: OFFICIAL: Sensitive (including when used with IMMs) and PROTECTED				
Classification and Information Management Marker (IMM)	**Examples**	**PERMITTED** / **NOT PERMITTED** **Use, Store and Transmit ON**		**PERMITTED to Distribute TO (Transmit To / Share With)**
OFFICIAL: Sensitive with Legislative Secrecy IMM **This is a security classification**	Information that is protected by specific secrecy provisions in legislation. Examples: • Commentaries on draft Bills not yet publicly released • Legislative bid documents – draft amendments Note: this information may instead be PROTECTED – **see Table 3** *Refer also to the PM&C Cabinet Handbook*	**Network:** The Office's Main Network Fortress **Record In:** Resolve Objective TechOne (for finance or procurement documents only) Fortress SharePoint	The Office's Public Websites or Social Media	Need-to-Know principle applies **OFFICIAL: Sensitive // Legislative Secrecy** marking to be displayed **Internal recipients**: Office personnel **External recipients**: Australian Government entities and personnel, prescribed private sector organisations and higher education institutions we oversee **External recipients**: non-Australian Government organisations or individuals – **ONLY** where there is an agreement or arrangement in place, such as a contract or deed, that establishes handling requirements and protections **UNLESS** the Office is returning or responding to information provided by a person or organisation outside of government, or their authorised representative, which the Office subsequently classified as OFFICIAL: Sensitive

Table 3: Security-classified information: OFFICIAL: Sensitive (including when used with IMMs) and PROTECTED				
Classification and Information Management Marker (IMM)	**Examples**	**PERMITTED** Use, Store and Transmit ON	**NOT PERMITTED** Use, Store and Transmit ON	**PERMITTED to Distribute TO (Transmit To / Share With)**
 PROTECTED **This is a security classification** Staff are directed to the Guidance – Use of Fortress for PROTECTED information for more information	Information that if compromised could cause damage to the national interest, organisations or individuals. Damage in this context could be reputational, financial or legal, exposing vulnerabilities in government operations or undermining diplomatic relations. Damage to an individual could be exposure to physical risk. Examples: • Cabinet documentation where premature disclosure could undermine Cabinet confidentiality and public trust • Operational Risk Assessments revealing vulnerabilities in critical infrastructure or emergency response plans • Sensitive procurement evaluations that disclose commercial-in-confidence details that could affect market fairness or integrity • Internal fraud investigation reports containing allegations, evidence and personal data that could harm reputations or legal standing *Refer also to the PM&C Cabinet Handbook*	**Network:** Fortress **Record In:** Fortress SharePoint	The Office's Main network is **not accredited** for the processing, storage or transmission of information at or above PROTECTED level and this includes all systems The Office's Public Websites or Social Media	Need-to-Know principle applies Information classified as PROTECTED must display the **PROTECTED** marking Recipients must be on a certified PROTECTED system Recipients must hold an appropriate security clearance

Appendix C: Privacy Act 1998 definition of personal information

The term 'personal information' encompasses a broad range of information.

A number of different types of information are explicitly recognised as constituting personal information under the Privacy Act. For example, the following are all types of personal information:

- 'sensitive information' (includes information or opinion about an individual's racial or ethnic origin, political opinion, religious beliefs, sexual orientation or criminal record, provided the information or opinion otherwise meets the definition of personal information)
- 'health information' (which is also 'sensitive information')
- 'credit information'
- 'employee record' information (subject to exemptions), and
- 'tax file number information'.

Although not explicitly recognised as personal information under the Privacy Act, information may be explicitly recognised as personal information under other legislation. For example, under the Telecommunications (Interceptions and Access) Act 1979 (Cth), certain telecommunications data (sometimes referred to as 'metadata') is taken to be personal information for the purposes of the Privacy Act.

However, information does not have to be explicitly recognised as personal information to constitute personal information under the Privacy Act. The types of information that are personal information are unlimited and can vary widely.

Further, the definition of personal information is not limited to information about an individual's private or family life but extends to any information or opinion that is about the individual, from which they are reasonably identifiable. This can include information about an individual's business or work activities.

Personal information can range from sensitive and confidential information to information that is publicly available. The definition also makes clear that information will be personal information even if it is incorrect.

Source: Excerpted from page titled What is personal information? – Office of the Australian Information Commissioner (OAIC) website, accessed 10 September 2025

Quick Guide to Classifying Information in the Office

This table, titled 'Quick Guide to Classifying Information in the Office', reproduces Appendix A of the Guidance – Classifying and Distributing Office Information, which was endorsed by the Chief Information Officer, Office of the Commonwealth Ombudsman (Office), for release to the Office's internal platform VOLT, in September 2025 (and for re-release to VOLT in January 2026).

Always follow the ***Need-to-Know*** principle of only accessing and transmitting information where there is a requirement to do so to fulfil official duties.

Classification and IMM	Examples	Distribute To (Transmit To / Share With)
UNOFFICIAL Does not relate to official duties	• A shopping list • Personal reminder • Organising lunch	No restrictions
OFFICIAL Most of our routine information	• General administration and correspondence • Team/branch presentations • Policies, procedures, guidance • Training materials • Publicly released reports • Social Media Content • Position Descriptions/Job Adverts	***Need-to-Know*** principle recommended
OFFICIAL: Sensitive without IMMs Information that requires additional care due to its sensitivity, and could cause limited damage to an individual, organisation or government generally if compromised	• EC, ITGC, ARC papers & minutes • Risk assessments • Branch at a Glance (BaaG) reports • Sensitive case handling • Sensitive investigations • Sensitive internal reports • Senate Estimates briefings • Security Incidents correspondence	***Need-to-Know*** principle applies **Internal recipients**: Office personnel **External recipients**: Australian Government entities and personnel, prescribed private sector organisations and higher education institutions we oversee **Other External recipients**: non-Australian Government organisations or individuals – *ONLY where there is an agreement or arrangement in place*, such as a contract or deed, that establishes handling requirements and protections **UNLESS** the Office is returning or responding to information provided by a person or organisation outside of government, or their authorised representative, which the Office subsequently classified as OFFICIAL: Sensitive
OFFICIAL: Sensitive Personal Privacy IMM OFFICIAL: Sensitive Information that contains personal information in accordance with the Privacy Act	• Documents or correspondence containing personal information about complainants or staff • Conflict of Interest declarations • PDA-related correspondence • Recruitment shortlists & evaluations • WHS Incident Reports	
OFFICIAL: Sensitive Legislative Secrecy IMM	• Draft Bills and draft legislation • Discussion about legislative amendments	
OFFICIAL: Sensitive Legal Privilege IMM	• Requests/instructions for legal advice • Draft or final legal advice • Legal briefings that contain legal advice	***Need-to-Know*** principle applies **All recipients**: Information that is classified OFFICIAL: Sensitive // Legal Privilege **requires the express permission of the Office's Legal Team** before distribution between parties
PROTECTED Information that if compromised could potentially damage the national interest, organisations or individuals	• Commonwealth Budget proposals • Office inspections of law enforcement agencies or places of detention • Analysis of proposed responses to recommendations made in parliamentary committee reports • Cyber Security Post Incident Reports	***Need-to-Know*** principle applies Distributed through Fortress to another certified PROTECTED level system Personnel that hold appropriate security clearances