



Security Classification Reforms

All official information requires an appropriate degree of protection—any deliberate or accidental compromise¹ of information could adversely affect government business. The PSPF defines the Australian Government's security classifications and associated handling protections.

How to handle sensitive and security classified information

Key operational controls to protect sensitive and security classified information include:

- a. identifying sensitive and security classified information
 - i. with a protective marking
 - ii. by creating an auditable record of all incoming and outgoing material, transfer, copy or movements for, at a minimum, TOP SECRET information and other accountable material
- b. limiting disclosure or access to sensitive and security information to personnel with:
 - i. a demonstrated need-to-know the content of the information
 - ii. an applicable security clearance
- c. transferring and transmitting information by means which deter and detect unauthorised access
- d. storing and using information securely
- e. destroying and disposing of information by secure means.

A. What has changed?

The reforms simplify the existing classification system as follows:

Then		Now
TOP SECRET	Security classifications	TOP SECRET
SECRET		SECRET
CONFIDENTIAL		N/A
PROTECTED		PROTECTED
Sensitive: Cabinet	DLM → Caveat	CABINET (Caveats can only be applied to security classified information, ie PROTECTED or above)
Sensitive	DLM → Information management marker	Apply classification or OFFICIAL: Sensitive and optional information management markers: <ul style="list-style-type: none"> • Legislative secrecy • Personal privacy • Legal privilege
Sensitive: Personal		
Sensitive: Legal		
For Official Use Only	DLM → DLM	OFFICIAL: Sensitive
UNCLASSIFIED	Non-classification markings	OFFICIAL
UNOFFICIAL		UNOFFICIAL

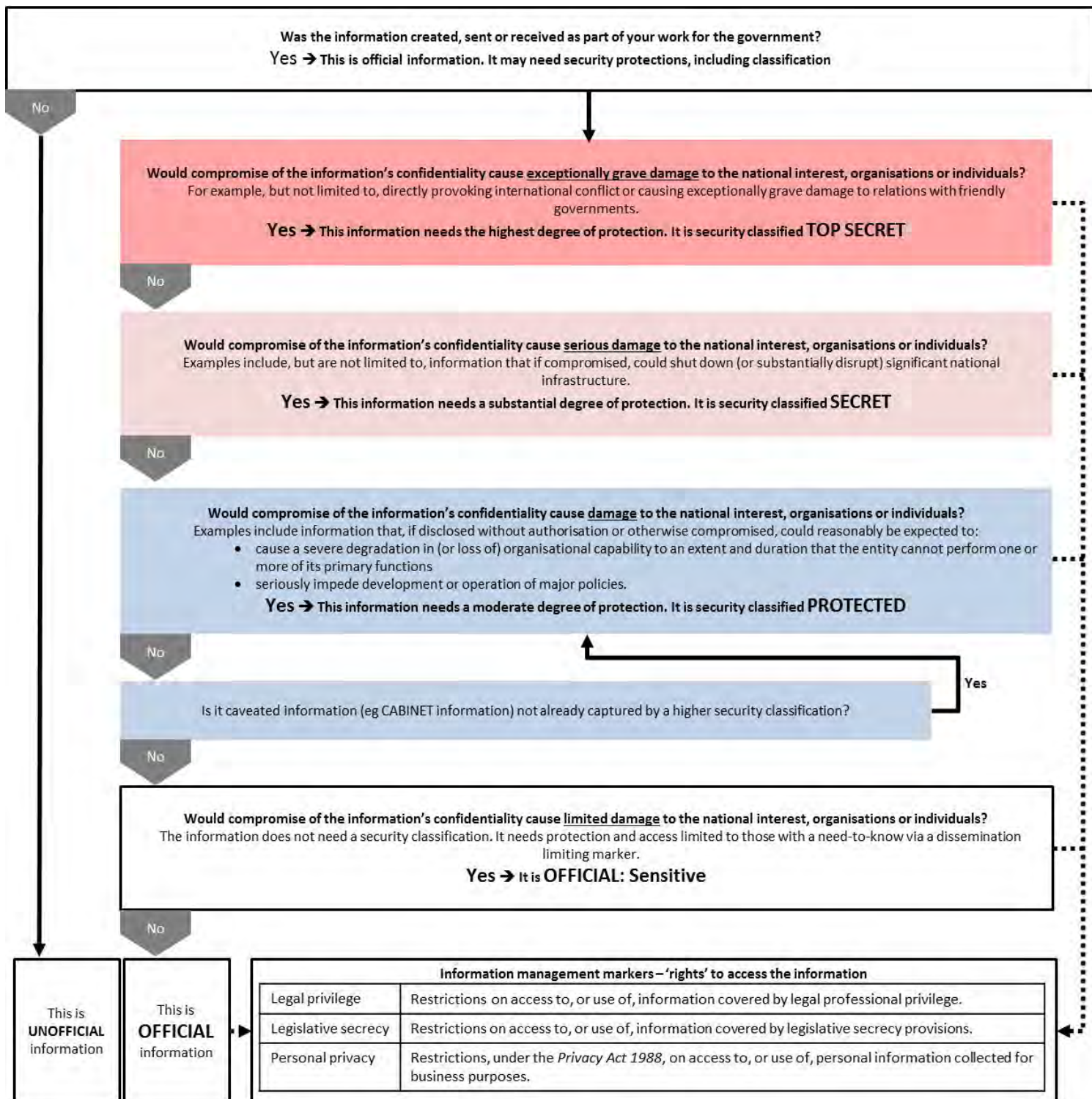
These changes are reflected in the new [Email protective marking standard](#) at Annex A of the PSPF policy: Sensitive and classified information.

¹ Information compromise includes, but is not limited to: loss, misuse, interference, unauthorised access, unauthorised modification and unauthorised disclosure.

Entities retain the option to further categorise information using other information management markers aligning with the National Archives of Australia’s ‘rights’ property terms.

B. Assessing whether information is sensitive or security classified²

In order to determine what protective marking to use, the originator (author/creator of the information) assesses its sensitivity or security classification by considering the potential impacts to national interest, organisations or individuals that could arise from compromise of the information’s confidentiality.



² There are historical security classifications and other protective markings that no longer reflect Australian Government policy. For assistance in applying appropriate handling protections (and assessing damage to the national interest, organisations or individuals) to historical classifications, see Historical markings table.

The information management markers reflect the Australian Government Recordkeeping Metadata Standard's 'Rights' property. While categorising information content by non-security access restrictions is not mandated as a security requirement, the 'Rights' property provides a standard set of terms ensuring common understanding, consistency and interoperability across systems and government entities. For guidance, see the PSPF policy: [Access to information](#).

Transition timeframes and milestones

While entities can commence using the new classification system from 1 October 2018, there is an extended transition for these reforms—with full implementation required by 1 October 2020.

1 January 2019 is the collective government **start date** to accept and receive emails using the new classification system (while still retaining the ability to receive emails under the old system). Entities **must not** send and receive emails using the old classification system after 1 October 2020.

	1 October 2018	1 January 2019	1 October 2020
Implementation stage	<p>PSPF REFORMS 2018 COMMENCES</p> <p>Transition to new system commences.</p>	<p>NEW CLASSIFICATION SYSTEM³ STARTS</p> <p>Collective government <i>start date</i> to accept and receive emails under the new system.</p> <p>All entities must ensure that their systems will not block emails that are marked under either the new or old system.</p>	<p>OLD CLASSIFICATION SYSTEM⁴ CEASES</p> <p>Entities must not send or receive emails under the old system after this date.</p>
	<p>Entities commence preparations to implement the new system in accordance with PSPF Policy: Sensitive and classified information.</p> <p>Entities prepare their email systems to accept messages according to the new scheme and update supporting internal ICT systems.</p> <p>This includes establishing entity procedures, engaging with service providers and educating personnel on the new system.</p>	<p>During January 2019 to September 2020, entities:</p> <ul style="list-style-type: none"> continue to educate personnel/users on new arrangements shift to marking new documents with new PSPF arrangements grandfather current holdings of classified and DLM material—noting that existing holdings do not need to be reclassified (historical handling protections remain). 	<p>After 1 October 2020, entities must use the new classification system for both internal and external communication.</p> <p>Entities must not send or receive emails using markings under the old system after this date.</p>
Internal (entity) communication	<p>Send: old or new system</p> <p>Receive: old or new system</p>	<p>Send: old or new system</p> <p>Receive: old or new system</p>	<p>Send: only new system</p> <p>Receive: only new system</p>
External communication	<p>Send : only old system (must not send externally under new system)</p> <p>Receive: must accept old system</p>	<p>Send: old or new system</p> <p>Receive: must receive old and new system</p>	<p>Send: only new system</p> <p>Receive: only new system</p>

³ Old classification system is the [Australian Government Security classification System](#) (PSPF 2014)

⁴ New classification system is PSPF policy: [Sensitive and classified information](#) (PSPF 2018)

Markings due to cease 1 October 2020

For DLMs and classification markings due to cease on 1 October 2020, entities are strongly encouraged not to create new material using these markings after 1 January 2019. These markings must not be used after 1 October 2020.

Marking	Key dates	Replacement equivalency	Handling
CONFIDENTIAL classification	CONFIDENTIAL classification is discontinued from 1 October 2018. Recognition of the CONFIDENTIAL classification ceases on 1 October 2020.	None established. Consider the harm and apply corresponding security classification marking	Historical handling protections remain.
For Official Use Only (FOUO) dissemination limiting marker (DLM)	FOUO DLM replaced on 1 October 2018. Recognition of the FOUO DLM ceases on 1 October 2020.	FOUO is equivalent to the current OFFICIAL: Sensitive level.	Handling of FOUO information is as per PSPF requirements for OFFICIAL: Sensitive.
Sensitive DLM	Sensitive DLM replaced on 1 October 2018. Recognition of the Sensitive DLM ceases on 1 October 2020.	Unless otherwise classified, Sensitive is equivalent to the current OFFICIAL: Sensitive level. The (optional) <i>Legislative secrecy</i> information management marker may be applied.	Handling of Sensitive information is: <ul style="list-style-type: none"> a. if classified, as per the identified classification level b. if not classified, as per PSPF requirements for OFFICIAL: Sensitive.
Sensitive: Cabinet DLM	Sensitive: Cabinet DLM replaced on 1 October 2018. Recognition of the Sensitive: Cabinet DLM ceases on 1 October 2020.	The Sensitive: Cabinet DLM is equivalent to the current CABINET caveat.	Handling of Sensitive: Cabinet information is as per: <ul style="list-style-type: none"> a. the identified classification level and b. PSPF (and Security Caveats Guidelines) requirements for the CABINET caveat.
Sensitive: Legal DLM	Sensitive: Legal DLM replaced on 1 October 2018. Recognition of the Sensitive: Legal DLM ceases on 1 October 2020.	Unless otherwise classified, Sensitive: Legal is equivalent to the current OFFICIAL: Sensitive level. The (optional) <i>Legal privilege</i> information management marker may be applied.	Handling of Sensitive: Legal information is: <ul style="list-style-type: none"> a. if classified, as per the identified classification level b. if not classified, as per PSPF requirements for OFFICIAL: Sensitive.
Sensitive: Personal DLM	Sensitive: Personal DLM replaced on 1 October 2018. Recognition of the Sensitive: Personal DLM ceases on 1 October 2020.	Unless otherwise classified, Sensitive: Personal is equivalent to the current OFFICIAL: Sensitive level. The (optional) <i>Personal privacy</i> information management marker may be applied.	Handling of Sensitive: Personal information is: <ul style="list-style-type: none"> a. if classified, as per the identified classification level b. if not classified, as per PSPF requirements for OFFICIAL: Sensitive.

Historical markings (ceased 1 August 2012)

Historical marking	Key dates	Current equivalency	Handling
HIGHLY PROTECTED classification	Recognition of the HIGHLY PROTECTED classification ceased on 1 August 2012.	HIGHLY PROTECTED is equivalent to the current SECRET classification.	Handling of HIGHLY PROTECTED information is as per PSPF requirements for SECRET.
RESTRICTED classification	Recognition of the RESTRICTED classification ceased on 1 August 2012.	RESTRICTED is equivalent to the current OFFICIAL: Sensitive level.	Handling of RESTRICTED information is as per PSPF requirements for OFFICIAL: Sensitive.
X-IN-CONFIDENCE classification	Recognition of the X-IN-CONFIDENCE classification ceased on 1 August 2012.	X-IN-CONFIDENCE is equivalent to the current OFFICIAL: Sensitive level.	Handling of X-IN-CONFIDENCE information is as per PSPF requirements for OFFICIAL: Sensitive.