Assessing Information

Press the **F5** button on your **keyboard** to begin.

Whether you work in Defence or with Defence, you are accountable for ensuring Official Information is treated with the highest level of integrity, accountability and security.

You are also accountable to assess your information appropriately to ensure it is properly protected and easily accessible by the people who need it.

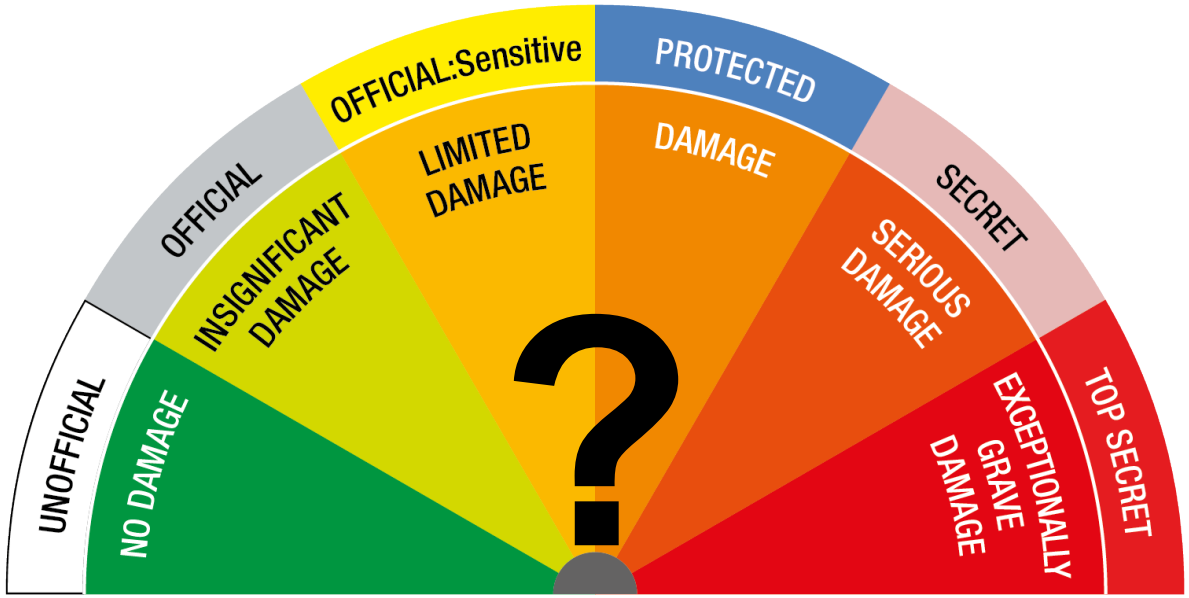
NEXT

Assessing Information

Information is a valuable resource and how we assess and protect it allows Defence to share and exchange information with confidence.

This interactive PowerPoint will help you to assess your information and apply an appropriate protective marker or classification.

Click the word '**HOME**' above at anytime, to return to this page.



NEXT

Assessing Information

When you create information, you are responsible for:

- **assessing the sensitivity of the information**
- **applying the appropriate protective marker or classification**
- **protecting the information appropriately.**

Has your information been created, sent or received as **part of your work** for Defence?

NO

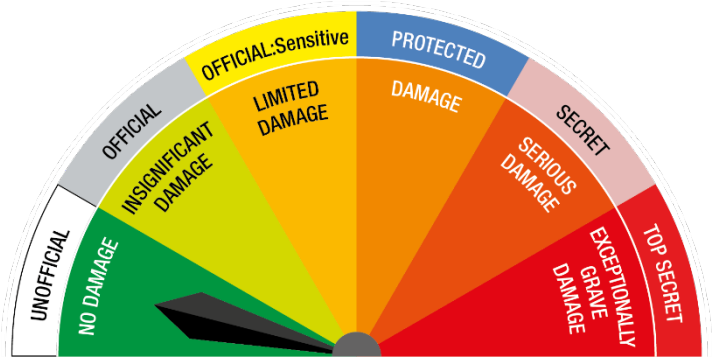
YES

UNOFFICIAL Information

Information relating to your home or personal life is **UNOFFICIAL** information.

Use this marker to identify Unofficial Information and emails when using the Defence emailing system.

Click here to find out how protective markers are applied to Official Information.



Examples include:

- an invitation to a birthday party
- calling your mechanic about a car service
- arranging tennis coaching for the weekend.

OFFICIAL Information

All information related to your work for Defence is **OFFICIAL** Information including:

- **briefs, letters, talking points, reports, presentations, memoranda, emails, and notes**
- **digital information stored on a computer, mobile or storage device**
- **all work related conversations in and away from the workplace.**

Now you need to assess the impact of your information.

NEXT

Assess the Damage

If your information was leaked or made public, what damage could it cause to people, organisations or government?

- **Insignificant damage**
- **Limited damage**
- **Moderate Damage**
- **Serious damage**
- **Exceptionally grave damage**

Select the most appropriate level to find out more details.

Business Impact Levels

Business Impact Levels (BILs) are used to identify the potential damage your information could cause to:

- **people,**
- **organisations** or
- **government**

By assessing the damage, you can determine the appropriate protective marker or classification.

Insignificant Damage

If your information was leaked or made public, it could cause:

- **Minor issues for routine business operations and diplomatic activities**
- **Minor impact to Defence assets or budget**
- **No issues with legislation, commercial confidentiality or legal requirements**

Does this damage level seem correct?

NO

YES

Limited Damage

If your information was leaked or made public, it could cause:

- **Defence's business functions to weaken**
- **$10M to $100M damage to Defence assets**
- **Minor loss of confidence in Government**
- **Suffering, harm or injury to someone, but not endanger their life**

Does this damage level seem correct?

NO

YES

Moderate Damage

If your information was leaked or made public, it could cause:

- **Disruption to one of Defence's main functions**
- **$100M to $10B damage to Defence assets or budget**
- **Major loss of confidence in Government**
- **Suffering or life threatening injury**

Does this damage level seem correct?

NO

YES

Serious Damage

If your information was leaked or made public, it could cause:

- **The disruption of all Defence functions**
- **Prevention of major policies**
- **Financial damage to an Australian industry sector**
- **Suffering and loss of life**

Does this damage level seem correct?

NO

YES

Exceptionally Grave Damage

If your information was leaked or made public, it could cause:

- **The collapse of political stability in Australia**
- **The collapse of the Australian economy**
- **The collapse of all major national infrastructure**
- **Widespread suffering and loss of life**

Does this damage level seem correct?

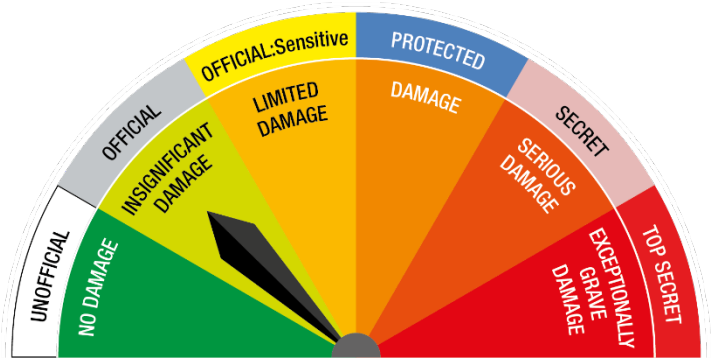
NO

YES

OFFICIAL

This means you should mark your information as OFFICIAL.

OFFICIAL has replaced UNCLASSIFIED as the protective marker to identify Official Information. The majority of Defence information created for routine business operations and services, is usually marked as OFFICIAL.



Examples include:

- hand written notes that you write at a Defence meeting
- an email to a work colleague about a Defence matter
- information prepared for public access or circulation, such as websites or Frequently Asked Questions.

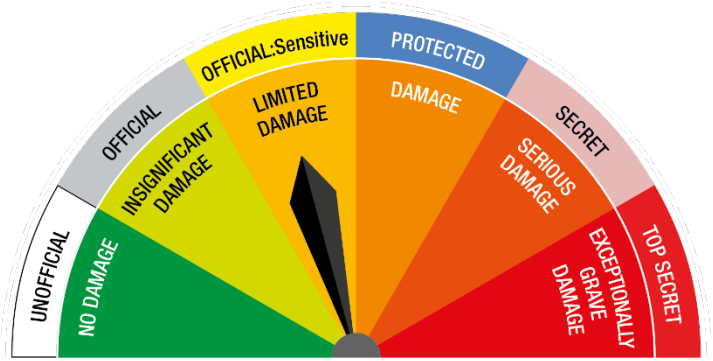
NEXT

OFFICIAL: Sensitive

This means you should mark your information as OFFICIAL: Sensitive.

OFFICIAL: Sensitive information is an attractive target because it is easier to access and a substantial amount of it exists.

The capture and assessment of a large amount of OFFICIAL: Sensitive information could reveal strategic intelligence about Defence personnel and operations.



Examples include:

- procurement details for a Defence Industry project
- standard operating procedures covering more sensitive internal workings.

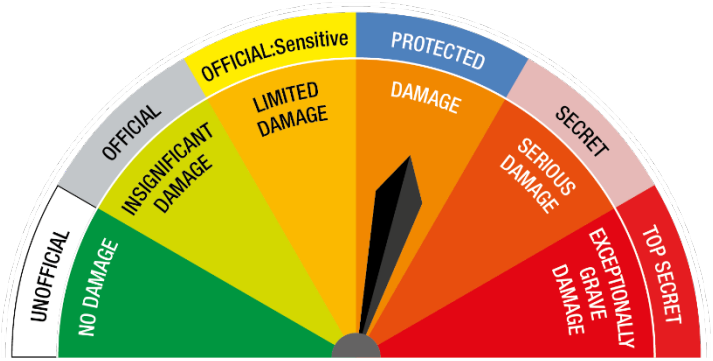
NEXT

PROTECTED

This means you should mark your information as PROTECTED.

PROTECTED information is an attractive target for domestic or international sources endeavouring to capture large amounts of information and data.

Aggregation of this information can reveal considerable details about the capabilities and movements of Defence assets.



Examples include:

- a Cabinet Submission
- a Movement Security Plan for domestic transport of weapons
- threat reports to support risk assessments for key events. e.g. ANZAC Day processions and movements of VIPs.

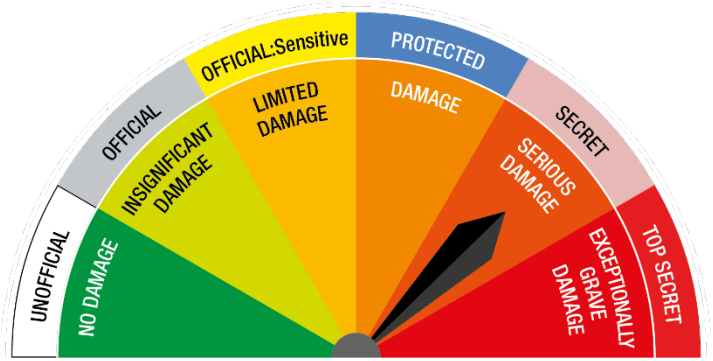
NEXT

SECRET

This means you should mark your information as SECRET.

SECRET information is a very attractive target that could reveal operational plans or strategies.

Appropriate measures must be taken and followed for creation, access, use, distribution and storage.



Examples include:

- highly sensitive technology unique and reserved for Australian use only
- tactical warfighting publications
- cryptographic and communications technology.

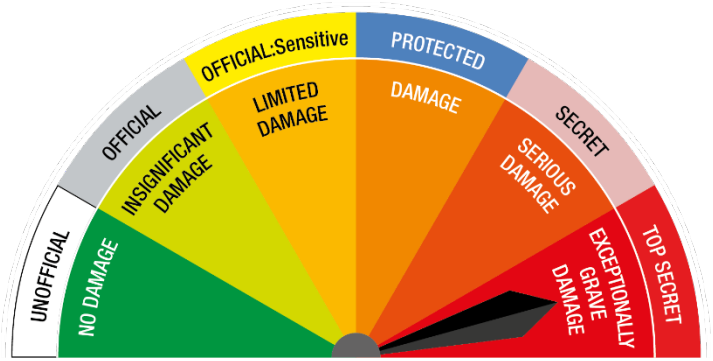
NEXT

TOP SECRET

This means you should mark your information as TOP SECRET.

TOP SECRET is the highest level of classified information used by Defence. It protects our most sensitive and valuable information.

Creation, access, use, replication and storage of TOP SECRET information must be strictly managed. This ensures the information is protected appropriately and prevents its unauthorised release or disclosure.



Examples include:

- intelligence information regarding foreign capabilities or operations
- operational plans
- sensitive capability plans.

NEXT

Other Markers

You can also use further markers to manage access and distribution of information.

Now you need to work out if you should apply an

- **Information Management Marker (IMM)** or a
- **Caveat Marker**

Select one to find out more information.

Information Management Markers (IMMs)

Use one of the three **IMMs** to indicate additional restrictions to information that have legislative protections. IMMs can be applied to information assessed as OFFICIAL: Sensitive or above.

- **Legal privilege** - to restrict access and use of information exchange between a lawyer and client for legal advice and proceedings.
- **Legislative secrecy** - to restrict access and use of information where rules for its release are specified in Commonwealth legislation.
- **Personal privacy** - to restrict access and use of personal information that is collected for business purposes as specified under the *Privacy Act 1988* (Cth).

Caveat Marker

Use a **Caveat Marker** to further restrict Classified information to people with a need-to-know or a need-to-access. Caveats can only be applied to information assessed as PROTECTED or above.

- **Special handling instructions (including Cabinet)**
- **Releasability caveats (AUSTEO, AGAO)**
- **Sensitive compartment information (Codewords)**

Select one to find out more information.

BACK FINISH

Special Handling Instructions

Use special handling instructions to indicate particular precautions for information handling.

CABINET – the only caveat allowed for PROTECTED information – identifies any material that:

- is prepared for the purpose of informing the Cabinet
- reveals the decisions and/or deliberations of the Cabinet
- is prepared by departments to brief their Minister's on proposals for Cabinet consideration
- has been created for the purpose of informing a proposal to be considered by the Cabinet.

EXCLUSIVE FOR (name of a person) caveat – identifies material intended for access by a named recipient, position title or designation only. This can only be applied to information assessed as SECRET or above.

BACK FINISH

Releasability Caveats

Use a Releasability Caveat to limit the release of information to a smaller audience. They can only be applied to information assessed as SECRET or above.

- **Releasable to** – identifies information which has been, or is releasable to the indicated foreign countries. It can only be used if Australia has a Security Information Agreement or whole-of-Government General Security Agreement with that country.
- **Australian Government Access Only (AGAO)** – indicates that only Australian Government employees can access the information. This Caveat is only used by Defence and a few other departments.
- **Australian Eyes Only (AUSTEO)** – indicates that only Australian citizens can access the information.

Codewords

Use a Codeword to identify a special need-to-know compartment. They can only be applied to information assessed as SECRET or above.

A Codeword is chosen so that its ordinary meaning is unrelated to the subject of the information. Standard compartment briefs include Charlie, Delta and Echo etc.

Access to Codeword or compartmented information requires additional briefings referred to as ‘compartment briefs’. The compartment briefs identify particular sensitivities of that information and any special rules that may apply, including the requirement for a certain security clearance level.

Finish

You have now completed the process of assessing Official Information.

The resources below will give you more information:

- online classification portal (also accessible by Defence industry)
- quick reference guides
- desktop awareness products
- training course updates, and
- Defence Service Desk knowledge articles

Defence personnel **Click here** Defence Industry **Click here**
to access these resources.

SUMMARY

Does the information relate to your work for Defence?

UNOFFICIAL Information

e.g. Email to organise weekend tennis lessons

Official Information

Classifications

Would compromise of this information cause **insignificant damage**?

OFFICIAL

e.g. A publicly accessible Defence website page

Would compromise of this information cause **limited damage**?

OFFICIAL: Sensitive

e.g. Procurement details for a Defence Industry project

Would compromise of this information cause **moderate damage**?

PROTECTED

e.g. Weapons movement report

Would compromise of this information cause **serious damage**?

SECRET

e.g. Operational military plans

Would compromise of this information cause **exceptionally grave damage**?

TOP SECRET

e.g. Intelligence report on a foreign country

Add Information Management Marker (IMM)

Add Caveat Marker