Significant Security Incidents

The Protective Security Policy Framework (PSPF) policy: Management structure and responsibilities requires entities to investigate, respond to and report on security incidents to the relevant authority or affected entity.

PSPF Policy: Management structures and responsibilities—requirements for significant security incidents

Core requirement – The accountable authority must …

b. empower the CSO to make decisions about:

iv. investigating, responding to, and reporting on security incidents.

Supporting Requirement 3 – Reporting security incidents

Entities must report significant security incidents to the relevant authority or affected entity, including informing the Attorney-General's Department of significant security incidents.

Security incidents

A security incident may have wide-ranging and critical consequences for a single entity or more broadly the Australian Government. In recognition of the potential consequences, managing security incidents is an important function of the Chief Security Officer (CSO).

The PSPF defines a ***security incident*** as:

- an **action** whether deliberate, reckless, negligent or accidental, that fails to meet protective security requirements or entity-specific protective security practices and procedures, and that results, or may result in, the loss, damage, corruption or disclosure of official information or resources
- an **approach** from anybody seeking unauthorised access to official resources
- an observable **occurrence or event** (including natural disaster events, terrorist attacks etc) that can harm Australian Government people, information or assets.

Significant security incidents

Generally, a significant security incident is one that is considered to be serious or complex.

The PSPF defines a ***significant security incident*** as a deliberate, negligent or reckless action that leads, or could lead, to the loss, damage, compromise, corruption or disclosure of official resources.

The CSO is responsible for managing the entity's response to security-related crises, incidents and emergencies in accordance with the entity's security incident and investigation procedures, and establishing monitoring mechanisms across the entity (refer Investigating, responding to and reporting on security incidents). This includes determining when a security incident is considered significant and therefore reportable.

How to determine a significant security incident

To determine whether a security incident is significant, the CSO (or their delegate) needs to consider whether the incident is a:

- ***Specified significant security incident*** that due to its nature is considered to be significant. Refer to the examples of significant security incidents in the security incident Tables 4 and 5 in PSPF Policy: Management structures and responsibilities.
- ***Significant business impact level security incident*** that due to the assessed severity of the potential or actual consequences or damage to the national interest, an organisation or individuals, is considered to be significant. A security incident assessed to have a Business Impact Level (BIL) of ***high***, ***extreme*** or

catastrophic is reportable, including to the Attorney-General's Department.
(Refer to Business Impact Levels Tool in PSPF Policy: Sensitive and classified information).

Diagram 1: Flowchart of CSO decision-making process to determine significant security incidents

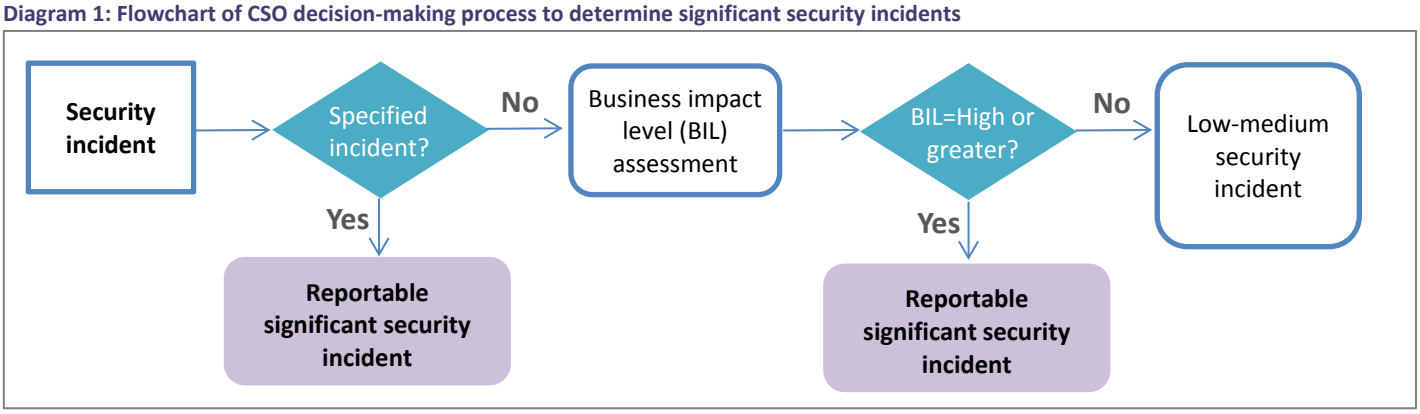

Table 1 Business impact level tool

Business impact level	Potential (or actual) harm to the national interest, organisations or individuals	Reportable to[1]
1 Low business impact	INSIGNFICANT DAMAGE	As per entity's procedures
2 Low to medium business impact	LIMITED DAMAGE	Entity's Chief Security Officer
3 High business impact	DAMAGE	Entity's Chief Security Officer + **Externally reportable**
4 Extreme business impact	SERIOUS DAMAGE	
5 Catastrophic business impact	EXCEPTIONALLY GRAVE DAMAGE	

How to report to Attorney-General's Department

All significant security incidents must be reported to the Attorney‑General's Department as they arise. Use the Significant security incident report template to report an incident to the Attorney-General's Department in accordance with advice provided in Table 2.

Table 2 Reporting significant security incidents to Attorney-General's Department

Security incident classification	Attorney-General's Department contact	Contact details
OFFICIAL, OFFICIAL: Sensitive or PROTECTED	Email the report template to the Director, Protective Security Policy	Email: PSPF@ag.gov.au
SECRET or TOP SECRET	Phone the PSPF Team for advice	Phone: (02) 6141 3600

This reporting obligation is in addition to the PSPF annual security report obligations for entities to provide a summary of significant security incidents during the reporting period. See the PSPF policy: Reporting on security.

For police, fire or ambulance response to a life threatening emergency or if a crime is in progress, call emergency services on triple zero (000).

Critical incidents that may affect public safety and require a coordinated response, call Australian Government Crisis Coordination Centre via the National Security Hotline on 1800 123 400.

Email PSPF@ag.gov.au or phone 02 6141 3600

[1] Refer to Table 5 of PSPF policy: Management structures and responsibilities for information on where to report for externally reportable incidents.