Reportable incident	Entity obligation to report	Reportable to
Significant security incidents	Advise the Attorney-General's Department of significant security incidents as they arise.	**Attorney-General's Department** PSPF Reporting Portal: https://portal.protectivesecurity.gov.au/ Email: PSPF@ag.gov.au Phone: 02 6141 3600 (PSPF Hotline)
National security incidents	Report security incidents or situations that have, or could have, an impact on national security, as defined in the *Australian Security Intelligence Organisation Act 1979* (ASIO Act), including suspected: a. espionage b. sabotage c. politically motivated violence d. promotion of communal violence e. attacks on Australia's defence system f. acts of foreign interference g. serious threats to Australia's territorial and border integrity. For security incidents that are reportable to ASIO, ASIO and the reporting entity will conduct an initial assessment of the potential harm. Dependent on the assessment, ASIO will either: recommend the entity continue with its own investigation and advise ASIO of the outcome, or conduct the investigation, in close consultation with the entity, and possibly in conjunction with the Australian Federal Police (AFP). Entities are encouraged to observe the need-to-know principle in relation to the details of a major security incident and its occurrence within an entity, until ASIO advises otherwise.	**Australian Security Intelligence Organisation** Email: asa@asio.gov.au Internet: http://www.asio.gov.au/ Phone: 13 ASIO (13 2746) (24hrs) For advice on whether the incident needs to be reported, contact the National Security Hotline on **1800 123 400**.
Cyber security incidents	Report any cyber security incidents relating to: a. suspicious or seemingly targeted emails with attachments or links b. any compromise or corruption of information c. unauthorised access or intrusion into an ICT system d. any viruses e. any disruption or damage to services or equipment data spills f. theft or loss of electronic devices that have processed or stored Australian Government information g. denial of service attacks h. suspicious or unauthorised network activity. To avoid inadvertently compromising any investigation into a cyber security incident, entities are encouraged to contact the ACSC as early as possible. Refer to Australian Government Information Security Manual: a. ISM security control 0123 – Cyber security incidents are reported to an organisation's CISO, or one of their delegates, as soon as possible after they occur or are discovered. b. ISM security control 0141 – When organisations use outsourced information technology or cloud services, their service providers report all cyber security incidents to the organisation's CISO, or one of their delegates, as soon as possible after they occur or are discovered.	**Australian Cyber Security Centre in Australian Signals Directorate** Email: asd.assist@defence.gov.au Form to report: https://www.cyber.gov.au/report Phone: Cyber Security Hotline: **1300 CYBER 1 (1300 292 371)**

	c. ISM security control 0140 – Cyber security incidents are reported to the ACSC.	
Cabinet material	Report security incidents (or suspected incidents) involving Cabinet material. Refer to the Cabinet Handbook for information on handling of Cabinet documents.	**Cabinet Division, Department of the Prime Minister and Cabinet** via entity Cabinet Liaison Officers.
Contact reporting	Under the **Australian Government Contact Reporting Scheme**, government personnel are required to report when a contact, either official or social, with a foreign national seems suspicious, persistent or unusual in any respect, or becomes ongoing. Such contact should be reported irrespective of whether it occurs within or outside Australia. Foreign nationals may include, but are not limited to, embassy or foreign government officials, including trade or business representatives. It is not necessary to report contact as part of official meetings provided a formal corporate record is produced detailing the topics discussed. However, employees should complete a contact report where a foreign national seeks to establish social contact outside official meetings, and/or where the contact seems suspicious, persistent or unusual. Additionally, personnel should report where a person or group, regardless of nationality, seeks to obtain information they do not need to know in order to do their job.	**Australian Security Intelligence Organisation** Email: cr@asio.gov.au
Incidents involving security clearance subjects	Report security incidents involving security clearance subjects. The entity is required to notify their vetting agency, at the appropriate time, of any security incident that may be relevant to a person's suitability to hold a security clearance. The appropriate time will depend on the significance of the incident, whether it is subject to investigation and an assessment of the related personnel security risks.	**Vetting agency** For clearances issued by the Australian Government Security Vetting Agency (AGSVA) Avenue to report: Security Officer Dashboard Phone: 1800 640 450
Correspondence of security concern	Report correspondence received that may be of a security concern, including but not limited to: a. threat to use violence to achieve a political objective b. warning of imminent threats to specific individuals, groups, property or buildings.	Entity security advisors (or CSO) to assess and determine the appropriate law enforcement or national security entity to externally report the incident.
Incident affecting another entity	Report any security incidents or unmitigated security risks that affect another entity's people, information or assets, particularly where entities are co-located or are providing services to another entity.	Advise the accountable authority of the entity whose people, information or assets may be affected. Refer to the Australian Government Directory
Classified equipment and services	Report any security incidents involving SCEC-endorsed safe hand courier services (using form). Report (via email to **SCEC@SCEC.gov.au)** any security incidents involving: a. SCEC-approved products faults or failure b. Destruction services - National Association for Information Destruction (NAID) AAA Certification with PSPF endorsement c. SCEC Security Zone Consultants and SCEC approved locksmiths.	**Security Construction and Equipment Committee** Report SCEC-endorsed safe hand courier services: https://www.scec.gov.au/scec-endorsed-courier-incidents Report other incidents types via email: scec@scec.gov.au
Unauthorised foreign entity access to	Report any occurrences of Australian classified information and assets being shared with a foreign national or international entity without the protection of an appropriate agreement or arrangement.	Entity CSO to determine the appropriate channel to externally report the incident.

classified Australian information or assets	Refer to PSPF policy: Security governance for international sharing. International agreements or international arrangements may impose additional reporting and security violation handling requirements beyond those detailed in the PSPF.	CSO may also need to consider whether the incident requires reporting under another category in this table.
Compromise of foreign entity information or assets	Where a suspected security incident involves the compromise of information, or other resources, that originate from a foreign government or governments, entities must comply with the arrangements outlined in the agreement or arrangement under which the information was obtained. Where the foreign government information has been provided by another entity, inform the providing entity of the security incident as soon as possible. The providing entity may have obligations it needs to apply under an agreement or arrangement. Refer to PSPF policy: Security governance for international sharing.	Report the incident to the originating foreign government (or entity that provided the information) as soon as practicable, in accordance with the overarching agreement or arrangement.
Eligible data breaches	Report eligible data breaches, in accordance with the Notifiable Data Breaches scheme under Part IIIC of the *Privacy Act 1988*, to the OAIC. The scheme only applies to data breaches involving personal information that are likely to result in serious harm to any individual affected. These are referred to as 'eligible data breaches'. The Commissioner must be notified as soon as practicable through a statement about the eligible data breach. When an entity is aware of reasonable grounds to believe an eligible data breach has occurred, it is also obligated to promptly notify any individual at likely risk of serious harm.	**Australian Information Commissioner** Form to report: https://www.oaic.gov.au/NDBform
Potential criminal/serious incidents	Report incidents that may constitute a criminal offence. See the AFP website for advice on the type of criminal incidents that are reported to the AFP (Commonwealth), or the local police (state or territory crimes), or if an incident is best handled within an entity. Examples of Commonwealth crimes (report to AFP): a. theft from the Commonwealth government b. assault on a Commonwealth official c. threats against a Commonwealth official. Examples of state and territory crimes (report to local police) a. cybercrime – including online fraud, such as eBay and internet scams b. stalking – including online stalking c. threats – including threats by phone, email, social networking sites, forums etc.	**AFP** for Commonwealth crimes Internet: https://www.afp.gov.au Phone: 02 6131 3000 **Local police** for state or territory crimes Phone: 13 14 44 **Crime Stoppers** to anonymously provide information about a crime Phone: 1800 333 000
Critical incidents involving public safety	**For critical incidents requiring immediate response, in particular where lives are at risk, call emergency services on triple zero (000).** Report any critical incidents that may affect public safety and require a coordinated response in support of the Australian Government and/or state and territory governments relating to: a. assault, including armed or military style assault b. arson, including suspected arson c. assassination, including suspected assassination d. bombing, including suspected use of explosive ordnance or improvised explosive devices e. chemical, biological or radiological attack, including suspected attacks f. attack on the National Information Infrastructure or critical infrastructure g. violent demonstration involving serious disruption of public order	**Australian Government Crisis Coordination Centre** Email: hotline@nationalsecurity.gov.au Internet: National Security Hotline Phone: 1800 123 400 The Crisis Coordination Centre will advise the AFP, ASIO, local police and/or other entities as appropriate.

h. hijacking, including suspected hijacking
i. hostage situation, including suspected hostage situation
j. kidnapping, including suspected kidnapping
k. mail bomb, including suspected mail bomb
l. white powder incident, including real or significant hoax incidents.