Table 5 External security incident reporting or referral obligations

Reportable incident	Entity obligation to report	Reportable to
National security incidents	Security incidents or situations that have, or could, 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.[Note 1] 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.	Director-General Australian Security Intelligence Organisation (ASIO) Email: asa@asio.gov.au Internet: http://www.asio.gov.au/ Phone: 02 6249 6299 (24hrs) For advice on whether the incident needs to be reported, contact the National Security Hotline on **1800 123 400**.
Significant cyber security incidents	Significant issues with implementing the Information Security Manual strategies to mitigate cyber incidents, or suspected 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. Refer to Information Security Manual: a. ISM security control 0140 – Cyber security incidents are reported to the ACSC using the CSIR scheme. b. ISM security control 0141 – When information technology services and functions have been outsourced, service providers report all cyber security incidents that occur.	Director-General Australian Signals Directorate (ASD) To avoid inadvertently compromising any investigation into a cyber security incident, entities are encouraged to contact ACSC as early as possible. Form: Cyber Security Incident Report Form Email: asd.assist@defence.gov.au Internet: http://www.asd.gov.au/infosec Phone the Cyber Security Hotline: 1300 292 371
Significant security incidents	As mandated in **Requirement 3**, advise the Attorney-General's Department of significant security incidents as they arise. Noting that the PSPF annual security report also requires entities to provide a summary of significant security incidents during the reporting period. See the PSPF policy: Reporting on security.	Email: PSPF@ag.gov.au Phone: 02 6141 3600 (PSPF Hotline)

[1] ASIO and the reporting entity must conduct an initial assessment of the potential compromise and 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).

Reportable incident	Entity obligation to report	Reportable to
Eligible data breaches	The Notifiable Data Breaches scheme under Part IIIC of the *Privacy Act 1988* established requirements for entities in responding to data breaches. 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'. When an entity is aware of reasonable grounds to believe an eligible data breach has occurred, it is obligated to promptly notify individuals at likely risk of serious harm.	The Commissioner must also be notified as soon as practicable through a statement about the eligible data breach, using: Form: OAIC's Notifiable Data Breach Form
Cabinet material	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. embassy or foreign government officials within Australia b. foreign officials and foreign nationals outside Australia a. seems suspicious, persistent or unusual in any respect, or becomes ongoing. Foreign officials could include trade or business representatives. 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.	ASIO a. CSO submits report to ASIO via cr@asio.gov.au.
Incidents involving security clearance subjects	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.	Contact vetting agency. For clearances issued by the Australian Government Security Vetting Agency: via the Security Officer Dashboard or Phone: 1800 640 450

Reportable incident	Entity obligation to report	Reportable to
Potential criminal/serious incidents	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). 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 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.	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.
Correspondence of security concern	Correspondence received that may be of a security concern, including: a. threat to use violence to achieve a political objective b. warning of imminent threats to specific individuals, groups, property or buildings	Report to Australia's law enforcement and national security agencies.

Reportable incident	Entity obligation to report	Reportable to
Incident affecting another entity	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.	Accountable authority of the entity whose people, information or assets may be affected. Refer to the Australian Government Directory
Classified equipment and services	Incidents involving SCEC services and ASIO approved destruction services.	Email: scec@scec.gov.au Form: SCEC courier incident report
Unauthorised foreign entity access to classified Australian information or assets	Inappropriately sharing classified Australian information and assets with a foreign national or international entity, without the protection of an agreement or arrangement. [Note 2] Refer to PSPF policy: Security governance for international sharing	Report to entity CSO (or security advisor) in line with internal reporting procedures. The incident may need to be externally reported – refer to other categories in this table.
Compromise of foreign entity information or assets	Failing to safeguard sensitive or security classified foreign entity information or assets covered by an international agreement or arrangement. Refer to PSPF policy: Security governance for international sharing	Report to entity CSO (or security advisor) in line with internal reporting procedures. The incident should be reported to the originating foreign government as soon as practicable.

[2] International agreements or international arrangements may impose additional reporting and security violation handling requirements beyond those detailed in the PSPF.