PSPF Release 2025 (July 2025) - List of Requirements						Status	PSPF Reporting		
Req Number	Release 25 Requirement	Domain	Section	Applicability (All, Dept of State, Security Service Provider Entity, Technical Authority Entity, Authorised Vetting Agency)	Start Date	Decision (Retain, Modify, Retire, New)	Question Type	Question Mandatory/ Not Mandatory	Question Scored/unscored
1	The Department of State supports portfolio entities to achieve and maintain an acceptable level of protective security through advice and guidance on government security.	GOV	01. WoAG Protective Security Roles	DOS	31/10/2024	Retain	Performance	Mandatory - only for DOS	Scored
2	The Accountable Authority complies with all Protective Security Directions.	GOV	01. WoAG Protective Security Roles	All entities	31/10/2024	Retain	Yes/No	Mandatory	Scored
3	The Technical Authority Entity provides technical advice and guidance to support entities to achieve and maintain an acceptable level of protective security.	GOV	01. WoAG Protective Security Roles	Technical Authority Entity	31/10/2024	Retain	Performance	Mandatory - only for TAE	Scored
4	The Shared Service Provider Entity supplies security services that help relevant entities achieve and maintain an acceptable level of security.	GOV	01. WoAG Protective Security Roles	Shared Service Provider Entity	31/10/2024	Retain	Performance	Mandatory - only for SSPE	Scored
5	The Shared Service Provider Entity develops, implements and maintains documented responsibilities and accountabilities for partnerships or security service arrangements with other entities.	GOV	01. WoAG Protective Security Roles	Shared Service Provider Entity	31/10/2024	Retain	Performance	Mandatory - only for SSPE	Scored
6	The Accountable Authority is answerable to their minister for the entity's protective security.	GOV	02. Entity Protective Security Roles and Responsibilities	All entities	31/10/2024	Retain	Yes/No	Mandatory	Scored
7	The Accountable Authority is responsible for managing the security risks of their entity.	GOV	02. Entity Protective Security Roles and Responsibilities	All entities	31/10/2024	Retain	Yes/No	Mandatory	Scored
8	A Chief Security Officer is appointed and empowered to oversee the entity's protective security arrangements.	GOV	02. Entity Protective Security Roles and Responsibilities	All entities	31/10/2024	Retain	Yes/No	Mandatory	Scored
9	The Chief Security Officer is a Senior Executive Service officer and holds a minimum security clearance of Negative Vetting 1.	GOV	02. Entity Protective Security Roles and Responsibilities	All entities	31/10/2024	Retain	Yes/No	Mandatory	Scored
10	The Chief Security Officer is accountable to the Accountable Authority for protective security matters.	GOV	02. Entity Protective Security Roles and Responsibilities	All entities	31/10/2024	Retain	Yes/No	Mandatory	Scored
11	A Chief Information Security Officer is appointed to oversee the entity's cyber security program and the cyber security for the entity's most critical technology resources .	GOV	02. Entity Protective Security Roles and Responsibilities	All entities	1/07/2025	Modify	Yes/No	Mandatory	Scored
12	The Chief Information Security Officer has the appropriate capability and experience and holds a minimum security clearance of Negative Vetting 1.	GOV	02. Entity Protective Security Roles and Responsibilities	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
13	The Chief Information Security Officer is accountable to the Accountable Authority for cyber security risks and how the entity's cyber security program is managing these risks.	GOV	02. Entity Protective Security Roles and Responsibilities	All entities	1/07/2025	Modify	Yes/No	Mandatory	Scored
14	Where appointed, security practitioners are appropriately skilled, empowered and resourced to perform their designated functions.	GOV	02. Entity Protective Security Roles and Responsibilities	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
15	Where appointed, security practitioners have access to training across government to maintain and upskill on new and emerging security issues.	GOV	02. Entity Protective Security Roles and Responsibilities	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
16	The Accountable Authority approves security governance arrangements that are tailored to the entity's size, complexity and risk environment.	GOV	02. Entity Protective Security Roles and Responsibilities	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
17	A dedicated security email address is established and monitored as the central conduit for distribution of protective security-related information across the entity.	GOV	02. Entity Protective Security Roles and Responsibilities	All entities	31/10/2024	Retain	Yes/No	Mandatory	Scored
18	A security plan is developed, implemented and maintained to address the mandatory elements of the plan.	GOV	03. Security Planning, Incidents and Training	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
19	The Accountable Authority approves the entity's security plan.	GOV	03. Security Planning, Incidents and Training	All entities	31/10/2024	Retain	Yes/No	Mandatory	Scored
20	The security plan is considered annually and reviewed at least every two years to confirm its adequacy and ability to adapt to shifts in the entity's risk, threat or operating environment.	GOV	03. Security Planning, Incidents and Training	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
21	Procedures are developed, implemented and maintained to ensure all elements of the entity's security plan are achieved.	GOV	03. Security Planning, Incidents and Training	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
22	Develop, establish and implement security monitoring arrangements to identify the effectiveness of the entity's security plan and establish a continuous cycle of improvement.	GOV	03. Security Planning, Incidents and Training	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
23	The Accountable Authority and Chief Security Officer develop, implement and maintain a program to foster a positive security culture in the entity and support the secure delivery of government business.	GOV	03. Security Planning, Incidents and Training	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
24	Security awareness training is provided to personnel, including contractors, at engagement and annually thereafter.	GOV	03. Security Planning, Incidents and Training	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
25	Targeted security training is provided to personnel, including contractors, in specialist or high-risk positions.	GOV	03. Security Planning, Incidents and Training	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
26	Procedures are developed, implemented and maintained to ensure security incidents are responded to and managed.	GOV	03. Security Planning, Incidents and Training	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
27	Security incident management and response plans are incorporated into the entity's business continuity arrangements.	GOV	03. Security Planning, Incidents and Training	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
28	Significant or externally reportable security incidents and referral obligations are reported to the relevant authority (or authorities) within the applicable timeframe.	GOV	03. Security Planning, Incidents and Training	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
29	Procedures are developed, implemented and maintained to investigate security incidents in accordance with the principles of the Australian Government Investigations Standards.	GOV	03. Security Planning, Incidents and Training	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
30	The principles of procedural fairness are applied to all security investigations, with due regard to national security considerations	GOV	03. Security Planning, Incidents and Training	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
31	The annual protective security report is provided to the entity's Minister.	GOV	04. Protective Security Reporting	All entities	31/10/2024	Retain	Yes/No	Mandatory	Scored
32	The annual protective security report is submitted to the Department of Home Affairs.	GOV	04. Protective Security Reporting	All entities	31/10/2024	Retain	Yes/No	Mandatory	Scored
33	The Accountable Authority approves the entity's annual protective security report and confirms that they have verified the report's content.	GOV	04. Protective Security Reporting	All entities	31/10/2024	Retain	Yes/No	Mandatory	Scored
34	Entities cooperate with the Department of Home Affairs' assurance activities to review annual protective security reports.	GOV	04. Protective Security Reporting	All entities	31/10/2024	Retain	Yes/No/NA	Mandatory	Scored
35	The annual Cyber Security Survey is submitted to the Australian Signals Directorate.	GOV	04. Protective Security Reporting	All entities	31/10/2024	Retain	Yes/No	Mandatory	Scored
36	The Accountable Authority determines their entity's tolerance for security risks and documents in the security plan.	RISK	05. Security Risk Management	All entities	31/10/2024	Retain	Yes/No	Mandatory	Scored
37	A risk steward (or manager) is identified for each security risk or category of security risk, including shared risks.	RISK	05. Security Risk Management	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
38	The Accountable Authority considers the impact that their security risk management decisions could potentially have on other entities, and shares information on risks where appropriate.	RISK	05. Security Risk Management	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
39	The entity is accountable for the management of security risks arising from procuring goods and services and ensures procurement and contract decisions do not expose the entity or the Australian Government to an unacceptable level of risk.	RISK	06. Third Party Risk Management	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
40	Procurement, contracts and third-party outsourced arrangements contain proportionate security terms and conditions to ensure service providers, contractors and subcontractors comply with relevant PSPF Requirements and avoid exposing the entity or the Australian	RISK	06. Third Party Risk Management	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
41	Entity ensures service providers, contractors and subcontractors comply with relevant PSPF Requirements as detailed by the entity.	RISK	06. Third Party Risk Management	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
42	Contractual security terms and conditions require service providers to report any actual or suspected security incidents to the entity, and follow reasonable direction from the entity arising from incident investigations.	RISK	06. Third Party Risk Management	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
43	Government entities providing outsourced services provide IRAP assessment reports to the government entities consuming, or looking to consume, their services.	RISK	06. Third Party Risk Management	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
44	Contract security terms and conditions are monitored and reviewed to ensure the specified security controls, terms and conditions are implemented, operated and maintained by the contracted provider, including any subcontractors, over the life of a contract.	RISK	06. Third Party Risk Management	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
45	Contractual terms and conditions include appropriate security arrangements for the completion or termination of the contract.	RISK	06. Third Party Risk Management	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
46	Procurement and contract decisions consider the security risks before engaging providers operating under foreign ownership, control or influence, and in response to any developments during the contract period that may give rise to foreign ownership, control or influence risks.	RISK	06. Third Party Risk Management	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
47	Security risks arising from contractual arrangements for the provision of goods and services are managed, reassessed and adjusted over the life of a contract.	RISK	06. Third Party Risk Management	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
48	Secure and verifiable third-party vendors, providers, partners and associated services are used unless business operations require use, and the residual risks are managed and approved by the Chief Information Security Officer	RISK	06. Third Party Risk Management	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
49	Entities manage the security risks associated with engaging with foreign partners.	RISK	07. Countering Foreign Interference and Espionage	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
50	Personnel do not publicise their security clearance level on social media platforms, including employment-focused platforms such as LinkedIn.	RISK	07. Countering Foreign Interference and Espionage	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
51	An insider threat program is implemented by entities that manage Baseline to Positive Vetting security clearance subjects, to manage the risk of insider threat in the entity.	RISK	07. Countering Foreign Interference and Espionage	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
52	Where exceptional circumstances prevent or affect an entity's capability to implement a PSPF requirement or standard, the Accountable Authority may vary application, for a limited period of time, consistent with the entity's risk tolerance.	RISK	08. Contingency Planning	All entities	31/10/2024	Retain	Yes/No/NA	Mandatory	Scored
53	Decisions to vary implementation of a PSPF requirement or standard due to exceptional circumstances are documented in the entity's security plan.	RISK	08. Contingency Planning	All entities	31/10/2024	Retain	Yes/No/NA	Mandatory	Scored
54	Decisions to implement an alternative mitigation measure that meets or exceeds a PSPF requirement or standard are reviewed and reported annually.	RISK	08. Contingency Planning	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
55	A business continuity plan is developed, implemented and maintained to respond effectively and minimise the impacts of significant business disruptions to the entity's critical services and assets, and other services and assets when warranted by a threat and security risk assessment.	RISK	08. Contingency Planning	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
56	Plans for managing a broad range of emergencies are integrated within the business continuity plan.	RISK	08. Contingency Planning	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
57	Personnel who are likely to be impacted are notified if there is a heightened risk of an emergency.	RISK	08. Contingency Planning	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
58	The originator remains responsible for controlling the sanitisation, reclassification or declassification of official and security classified information, and approves any changes to the information's security classification.	INFO	09. Classifications and Caveats	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
59	The value, importance or sensitivity of official information (intended for use as an official record) is assessed by the originator by considering the potential damage to the government, the national interest, organisations or individuals that would arise if the information's confidentiality were compromised.	INFO	09. Classifications and Caveats	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
60	The security classification is set at the lowest reasonable level.	INFO	09. Classifications and Caveats	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
61	Security classified information is clearly marked with the applicable security classification, and when relevant, security caveat, by using text-based markings, unless impractical for operational reasons.	INFO	09. Classifications and Caveats	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
62	The minimum protections and handling requirements are applied to protect OFFICIAL and security classified information.	INFO	09. Classifications and Caveats	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
63	The Australian Government Security Caveat Standard and special handling requirements imposed by the controlling authority are applied to protect security caveated information.	INFO	09. Classifications and Caveats	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
64	Security caveats are clearly marked as text and only appear in conjunction with a security classification.	INFO	09. Classifications and Caveats	All entities	1/07/2025	Modify	Performance	Mandatory	Scored
65	Accountable material has page and reference numbering.	INFO	09. Classifications and Caveats	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
66	Accountable material is handled in accordance with any special handling requirements imposed by the originator and security caveat owner detailed in the Australian Government Security Caveat Standard.	INFO	09. Classifications and Caveats	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
67	The Australian Government Email Protective Marking Standard is applied to protect OFFICIAL and security classified information exchanged by email in and between Australian Government entities, including other authorised parties.	INFO	09. Classifications and Caveats	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
68	The Australian Government Recordkeeping Metadata Standard's 'Security Classification' property (and where relevant, the 'Security Caveat' property) is applied to protectively mark information on technology systems that store, process or communicate security classified information.	INFO	09. Classifications and Caveats	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
69	Apply the Australian Government Recordkeeping Metadata Standard's 'Rights' property where the entity wishes to categorise information content by the type of restrictions on access.	INFO	09. Classifications and Caveats	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
70	Security classified discussions and dissemination of security classified information are only conducted in approved locations.	INFO	09. Classifications and Caveats	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
71	Entity implements operational controls for its information holdings that are proportional to their value, importance and sensitivity.	INFO	10. Information Holdings	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
72	An auditable register is maintained for TOP SECRET information and accountable material.	INFO	10. Information Holdings	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
73	OFFICIAL and security classified information is disposed of securely in accordance with the Minimum Protections and Handling Requirements, Information Security Manual, the Records Authorities, a Normal Administrative Practice and the Archives Act 1983.	INFO	11. Information Disposal	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
74	Security classified information is appropriately destroyed in accordance with the Minimum Protections and Handling Requirements when it has passed the minimum retention requirements or reaches authorised destruction dates.	INFO	11. Information Disposal	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
75	Access to security classified information or resources is only provided to people outside the entity with the appropriate security clearance (where required) and a need-to-know, and is transferred in accordance with the Minimum Protections and Handling Requirements	INFO	12. Information Sharing	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
76	The Memorandum of Understanding between the Commonwealth, States and Territories is applied when sharing information with state and territory government agencies.	INFO	12. Information Sharing	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
77	An agreement or arrangement, such as a contract or deed, that establishes handling requirements and protections, is in place before security classified information or resources are disclosed or shared with a person or organisation outside of government, unless the entity is returning or responding to information provided by a person or organisation outside of government, or their authorised representative, which the government entity subsequently classified as OFFICIAL: Sensitive.	INFO	12. Information Sharing	All entities	1/07/2025	Modify	Performance	Mandatory	Scored
78	Provisions are met concerning the security of people, information and resources contained in international agreements and arrangements to which Australia is a party.	INFO	12. Information Sharing	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
79	Australian Government security classified information or resources shared with a foreign entity is protected by an explicit legislative provision, international agreement or international arrangement.	INFO	12. Information Sharing	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
80	Australian Government security classified information or resources bearing the Australian Eyes Only (AUSTEO) caveat is never shared with a person who is not an Australian citizen, even when an international agreement or international arrangement is in place, unless an exemption is granted.	INFO	12. Information Sharing	All entities	1/07/2025	Modify	Performance	Mandatory	Scored
81	Australian Government security classified information or resources bearing the Australian Government Access Only (AGAO) caveat is not shared with a person who is not an Australia citizen, even when an international agreement or international arrangement is in place, unless they are working for, or seconded to, an entity that is a member of National Intelligence Community, the Department of Defence or the Australian Submarine Agency.	INFO	12. Information Sharing	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
82	Where an international agreement or international arrangement is in place, security classified foreign entity information or resources are safeguarded in accordance with the provisions set out in the agreement or arrangement.	INFO	12. Information Sharing	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
83	Australian Government security classified information or resources shared with a foreign non-government stakeholder is protected by an explicit legislative provision, international agreement or international arrangement.	INFO	12. Information Sharing	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
84	The Australian Signals Directorate's Information Security Manual cyber security principles are applied during all stages of the lifecycle of each system	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
85	The Australian Signals Directorate's Information Security Manual controls and cyber security guidelines are applied on a risk-based approach.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
211	A Technology Asset Stocktake and Technology Security Risk Management Plan is created to identify and manage the entity's internet-facing systems or services is maintained to ensure continuous visibility and monitoring of the entity's resource and technology estate.	TECH	13. Technology Lifecycle Management	All entities	1/07/2025	New	Performance	Mandatory	Scored
86	The Authorising Officer authorises each technology system to operate based on the acceptance of the residual security risks associated with its operation before that system processes, stores or communicates government information or data.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
87	Decisions to authorise (or reauthorise) a new technology system or make changes to an existing technology system are based on the Information Security Manual's risk-based approach to cyber security.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
88	The technology system is authorised to the highest security classification of the information and data it will process, store or communicate.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
89	A register of the entity's authorised technology systems is developed, implemented and maintained, and includes the name and position of the Authorising Officer, system owner, date of authorisation, and any decisions to accept residual security risks.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
90	Each technology system's suitability to be authorised to operate is reassessed when it undergoes significant functionality or architectural change, or where the system's security environment has changed considerably.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
91	The TikTok application is prevented from being installed, and existing instances are removed, on government devices, unless a legitimate business reason exists which necessitates the installation or ongoing presence of the application.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	Retain	Yes/No	Mandatory	Scored

92	The Chief Security Officer or Chief Information Security Officer approves any legitimate business reason for the use of the TikTok application on government devices and ensures the following mitigations are in place to manage security risks: • Ensure the TikTok application is installed and accessed only on a separate, standalone device without access to services that process or access official and classified information. • Ensure the separate, standalone device is appropriately stored and secured when not in use. This includes the isolation of these devices from sensitive conversations and information. • Ensure metadata has been removed from photos, videos and documents when uploading any content to TikTok. • Minimise, where possible, the sharing of personal identifying content on the TikTok application. • Use an official generic email address (for example, a group mailbox) for each TikTok account. • Use multi-factor authentication and unique passphrases for each TikTok account. • Ensure that devices that access the TikTok application are using the latest available operating system in order to control individual mobile application permissions. Regularly check for and update the application to ensure the latest version is used. • Only install the TikTok application from trusted stores such as Microsoft Store, Google Play Store and the Apple App Store. • Ensure only authorised users have access to corporate TikTok accounts and that access (either direct or delegated) is revoked immediately when there is no longer a requirement for that access. • Carefully and regularly review the terms and conditions, as well as application permissions with each update, to ensure appropriate risk management controls can be put in place or adjusted as required. • Delete the TikTok application from devices when access is no longer needed.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	Retain	Yes/No/NA	Mandatory	Scored
93	The Australian Signals Directorate's temporary mitigations for legacy IT are applied to manage legacy information technology that cannot yet be replaced.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	Retain	Yes/No/NA	Mandatory	Scored
94	Technology assets and their components, classified as SECRET or below are stored in the appropriate Security Zone based on their aggregated security classification or business impact level.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
95	Technology assets and their components classified as TOP SECRET are stored in suitable SCEC-endorsed racks or compartments within an accredited Security Zone Five area meeting ASIO Technical Note 5/12 – Compartments within Zone Five areas requirements.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
96	Outsourced facilities that house technology assets and their components with a catastrophic business impact level are certified by ASIO-T4 physical security and accredited by ASD before they are used operationally.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
97	Technology assets are disposed of securely in accordance with the Information Security Manual.	TECH	13. Technology Lifecycle Management	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
212	Approved post-quantum cryptographic encryption algorithms are used for newly procured cryptographic equipment and software in accordance with the Information Security Manual's guidelines for cryptography.	TECH	13. Technology Lifecycle Management	All entities	1/07/2025	New	Performance	Mandatory	Scored
98	A cyber security strategy and uplift plan is developed, implemented and maintained to manage the entity's cyber security risks in accordance with the Information Security Manual and the Guiding Principles to Embed a Zero Trust Culture.	TECH	14. Cyber Security Strategies	All entities	1/07/2025	Modify	Performance	Mandatory	Scored
213	The Chief Information Security Officer reports on the entity's cyber security risk at each meeting of the Audit Committee and biannually on the progress of the cyber security strategy and uplift plan.	TECH	14. Cyber Security Strategies	All entities	1/07/2025	New	Yes/No	Mandatory	Scored
99	Patch applications mitigation strategy is implemented to Maturity Level Two under ASD's Essential Eight Maturity Model.	TECH	14. Cyber Security Strategies	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
100	Patch operating systems mitigation strategy is implemented to Maturity Level Two under ASD's Essential Eight Maturity Model.	TECH	14. Cyber Security Strategies	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
101	Multi-factor authentication mitigation strategy is implemented to Maturity Level Two under ASD's Essential Eight Maturity Model.	TECH	14. Cyber Security Strategies	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
102	Restrict administrative privileges mitigation strategy is implemented to Maturity Level Two under ASD's Essential Eight Maturity Model.	TECH	14. Cyber Security Strategies	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
103	Application control mitigation strategy is implemented to Maturity Level Two under ASD's Essential Eight Maturity Model.	TECH	14. Cyber Security Strategies	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
104	Restrict Microsoft Office macros mitigation strategy is implemented to Maturity Level Two under ASD's Essential Eight Maturity Model.	TECH	14. Cyber Security Strategies	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
105	User application hardening mitigation strategy is implemented to Maturity Level Two under ASD's Essential Eight Maturity Model.	TECH	14. Cyber Security Strategies	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
106	Regular back-ups mitigation strategy is implemented to Maturity Level Two under ASD's Essential Eight Maturity Model.	TECH	14. Cyber Security Strategies	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
107	The remaining mitigation strategies from the Strategies to Mitigate Cyber Security Incidents are considered and, where required, implemented to achieve an acceptable level of residual risk for their entity.	TECH	14. Cyber Security Strategies	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
108	A Protective Domain Name System service or other security mechanisms is used to prevent connections to and from known malicious endpoints.	TECH	15. Cyber Security Programs	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
109	Cloud Service Providers that have completed an IRAP assessment against the latest version of ASD's Information Security Manual within the previous 24 months are used.	TECH	15. Cyber Security Programs	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
110	Entities consider IRAP assessment recommendations and findings, and implement on a risk-based approach.	TECH	15. Cyber Security Programs	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
111	Security classified or systems of government significance information and data is securely hosted using a Cloud Service Provider and Data Centre Provider that has been certified against the Australian Government Hosting Certification Framework.	TECH	15. Cyber Security Programs	All entities	1/07/2025	Modify	Performance	Mandatory	Scored
112	The Data Centre Facilities Supplies Panel is used when procuring certified data centre space and services.	TECH	15. Cyber Security Programs	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
113	Internet-connected technology systems, and the data they process, store or communicate, are protected by a gateway in accordance with the Information Security Manual and the Gateways Policy.	TECH	15. Cyber Security Programs	All entities	31/10/2024	Retire	Performance	Mandatory	Scored
214	Digital Infrastructure that processes, stores or communicates Australian Government security classified information is protected by a Gateway or Security Service Edge in accordance with the Australian Government Gateway Security Standard.	TECH	15. Cyber Security Programs	All entities	1/07/2025	New	Performance	Mandatory	Scored
114	Gateways or Secure Service Edges that have completed an IRAP assessment (or ASD assessment for TOP SECRET gateways) against the latest version of ASD's Information Security Manual within the previous 24 months are used.	TECH	15. Cyber Security Programs	All entities	1/07/2025	Modify	Performance	Mandatory	Scored
115	A vulnerability disclosure program and supporting processes and procedures are established to receive, verify, resolve and report on vulnerabilities disclosed by both internal and external sources.	TECH	15. Cyber Security Programs	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
215	Participate in the Australian Signals Directorate's Cyber Security Partnership Program and notify ASD in the event of a change in the entity's risk profile.	TECH	15. Cyber Security Programs	All entities	1/07/2025	New	Yes/No	Mandatory	Scored
216	Connect to the Australian Signals Directorate's Cyber Threat Intelligence Sharing platform.	TECH	15. Cyber Security Programs	All entities	1/07/2025	New	Yes/No	Mandatory	Scored
217	Declared Systems of Government Significance are protected in accordance with the Australian Government Systems of Government Significance Standard.	TECH	15. Cyber Security Programs	SOGS	1/07/2025	New	Performance	Mandatory	Scored
116	The eligibility and suitability of personnel who have access to Australian Government people and resources is ensured.	PER	16. Pre-Employment Eligibility	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
117	The pre-employment screening identity check is conducted for all personnel, to verify identity to at least Level 3 (High) of Assurance of the National Identity Proofing Guidelines.	PER	16. Pre-Employment Eligibility	All entities (Note: does not apply to the staff of Ministers employed under Part III of the Members of Parliament (Staff) Act 1984	31/10/2024	Retain	Performance	Mandatory	Scored
118	Biographic information in identity documents is verified to ensure the information matches the original record.	PER	16. Pre-Employment Eligibility	All entities (Note: does not apply to the staff of Ministers employed under Part III of the Members of Parliament (Staff) Act 1984	31/10/2024	Retain	Performance	Mandatory	Scored
119	The pre-employment screening eligibility check is conducted for all personnel, to confirm their eligibility to work in Australia and for the Australian Government.	PER	16. Pre-Employment Eligibility	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
120	The entity obtains assurance of each person's suitability to access Australian Government resources, including their agreement to comply with the government's policies, standards, protocols and guidelines that safeguard resources from harm, during pre-employment screening.	PER	16. Pre-Employment Eligibility	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
121	Prior to granting temporary access to security classified information or resources, pre-employment checks are completed, and an existing Negative Vetting 1 security clearance is confirmed prior to granting temporary access to TOP SECRET information data or resources.	PER	17. Access to Resources	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
122	A risk assessment determines whether a person is granted temporary access to security classified information or resources.	PER	17. Access to Resources	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
123	Temporary access to security classified information, resources and activities is supervised.	PER	17. Access to Resources	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
124	Short-term temporary access to security classified information, resources and activities is limited to the period in which an application for a security clearance is being processed for the particular person, or up to a total combined maximum of three months in a 12-month period for all entities. *Note: 12-months refers to the preceding 12-months from the date the short-term access would be granted.*	PER	17. Access to Resources	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
125	The Authorised Vetting Agency confirms that the completed security clearance pack has been received, and that no initial concerns have been identified for the clearance subject, before short-term temporary access is changed to provisional temporary access.	PER	17. Access to Resources	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
126	Temporary access to classified caveated information, resources or activities is not granted, other than in exceptional circumstances, and only with the approval of the caveat controlling authority.	PER	17. Access to Resources	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
127	Prior to granting temporary access, the entity obtains an undertaking from the person to protect the security classified information, resources and activities they will access.	PER	17. Access to Resources	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
128	Prior to granting temporary access, the entity obtains agreement from any other entity (or third party) whose security classified information, resources and activities will be accessed by the person during the temporary access period.	PER	17. Access to Resources	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
129	Access to official information is facilitated for entity personnel and other relevant stakeholders.	PER	17. Access to Resources	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
130	Appropriate access to official information is enabled, including controlling access (including remote access) to supporting technology systems, networks, infrastructure, devices and applications.	PER	17. Access to Resources	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
131	Access to security classified information or resources is only given to entity personnel with a need-to-know that information.	PER	17. Access to Resources	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
132	Personnel requiring ongoing access to security classified information or resources are security cleared to the appropriate level.	PER	17. Access to Resources	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
133	Personnel requiring access to caveated information meet any clearance and suitability requirements imposed by the originator and caveat controlling authority.	PER	17. Access to Resources	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
134	A unique user identification, authentication and authorisation practice is implemented on each occasion where system access is granted, to manage access to systems holding security classified information.	PER	17. Access to Resources	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
135	A security risk assessment of the proposed location and work environment informs decisions by the Chief Security Officer to allow personnel to work in another government entity's facilities in Australia.	PER	17. Access to Resources	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
136	An agreement is in place to manage the security risks associated with personnel working in another government entity's facilities in Australia.	PER	17. Access to Resources	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
137	Approval for remote access to TOP SECRET information, data or systems in international locations outside of facilities meeting PSPF requirements is only granted if approved by the Australian Signals Directorate.	PER	17. Access to Resources	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
138	A security risk assessment of the proposed location and work environment informs decisions to allow personnel to work remotely in international locations.	PER	17. Access to Resources	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
139	Personnel are not granted approval to work remotely in locations where Australian Government information, or resources are exposed to extrajudicial directions from a foreign government that conflict with Australian law, unless operationally required, and the residual risks are managed and approved by the Chief Security Officer.	PER	17. Access to Resources	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
140	The Australian Government Security Vetting Agency (AGSVA) or the TOP SECRET-Privileged Access Vetting Authority is used to conduct security vetting, or where authorised, the entity conducts security vetting in a manner consistent with the Personnel Security Vetting Process and Australian Government Personnel Security Adjudicative Standard.	PER	18. Security Clearances	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
141	All vetting personnel attain and maintain the required skills and competencies for their role.	PER	18. Security Clearances	Authorised Vetting Agency	31/10/2024	Retain	Performance	Mandatory - only for AVA	Scored
142	The gaining sponsoring entity establishes new clearance conditions before assuming sponsorship of an existing security clearance that is subject to clearance conditions.	PER	18. Security Clearances	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
143	The gaining sponsoring entity undertakes the exceptional business requirement and risk assessment provisions prior to requesting transfer of sponsorship of an existing security clearance that is subject to an eligibility waiver.	PER	18. Security Clearances	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
144	The Authorised Vetting Agency only issues a security clearance where the clearance is sponsored by an Australian Government entity or otherwise authorised by the Australian Government.	PER	18. Security Clearances	All entities	31/10/2024	Retain	Performance	Mandatory - only for AVA	Scored
145	Positions that require a security clearance are identified and the level of clearance required is documented.	PER	18. Security Clearances	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
146	Each person working in an identified position has a valid security clearance issued by the relevant Authorised Vetting Agency.	PER	18. Security Clearances	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
147	Australian citizenship is confirmed and pre-employment screening is completed before the entity seeks a security clearance for a person in a position identified as requiring a security clearance.	PER	18. Security Clearances	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
218	The Sponsoring Entity ensures clearance subjects with an eligibility waiver or where a waiver is being considered, are not given temporary or provisional access to security classified information or resources until the security vetting process is complete.	PER	18. Security Clearances	All entities	1/07/2025	New	Performance	Mandatory	Scored
148	The Sponsoring Entity establishes an exceptional business need and conducts a risk assessment before a citizenship eligibility waiver is considered for a non-Australian citizen who has a valid visa and work rights to work in an identified position.	PER	18. Security Clearances	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
149	The Accountable Authority (or the Chief Security Officer if delegated) approves a citizenship eligibility waiver (after accepting the residual risk of waiving the citizenship requirement for that person, confirming that a checkable background eligibility waiver is not in place), and maintains a record of all citizenship eligibility waivers approved.	PER	18. Security Clearances	All entities	1/07/2025	Modify	Performance	Mandatory	Scored
150	The Sponsoring Entity establishes an exceptional business need and conducts a risk assessment (including seeking advice from the Authorised Vetting Agency), before a checkable background eligibility waiver is considered for a clearance subject assessed as having an uncheckable background.	PER	18. Security Clearances	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
151	The Sponsoring Entity's Accountable Authority (or the Chief Security Officer if delegated) approves checkable background eligibility waivers (after accepting the residual risk of waiving the checkable background requirement for each person and confirming that a citizenship eligibility waiver is not in place), and maintains a record of all checkable background eligibility waivers approved.	PER	18. Security Clearances	All entities	1/07/2025	Modify	Performance	Mandatory	Scored
152	The Authorised Vetting Agency provides the Sponsoring Entity with information to inform a risk assessment if a clearance subject has an uncheckable background and only issues a clearance if the Accountable Authority waives the checkable background requirement and provides the Authorised Vetting Agency with a copy of the waiver.	PER	18. Security Clearances	Authorised Vetting Agency	31/10/2024	Retain	Performance	Mandatory - only for AVA	Scored
153	The clearance subject's informed consent is given to collect, use and disclose their personal information for the purposes of assessing and managing their eligibility and suitability to hold a security clearance.	PER	19. Personnel Security Vetting Process	Authorised Vetting Agency	31/10/2024	Retain	Performance	Mandatory - only for AVA	Scored
154	The clearance subject's eligibility and suitability to hold a Baseline, Negative Vetting 1, Negative Vetting 2 or Positive Vetting security clearance is assessed by considering their integrity (i.e. the character traits of maturity, trustworthiness, honesty, resilience, tolerance and loyalty) in accordance with the Australian Government Personnel Security Adjudicative Standard.	PER	19. Personnel Security Vetting Process	Authorised Vetting Agency	31/10/2024	Retain	Performance	Mandatory - only for AVA	Scored
155	The clearance subject's eligibility and suitability to hold a TOP SECRET-Privileged Access security clearance is assessed in accordance with the TOP SECRET-Privileged Access Standard.	PER	19. Personnel Security Vetting Process	Authorised Vetting Agency	31/10/2024	Retain	Performance	Mandatory - only for AVA	Scored
156	The clearance subject's eligibility and suitability to hold a Baseline, Negative Vetting 1, Negative Vetting 2 or Positive Vetting security clearance is assessed by conducting the minimum personnel security checks for the commensurate security clearance level.	PER	19. Personnel Security Vetting Process	Authorised Vetting Agency	31/10/2024	Retain	Performance	Mandatory - only for AVA	Scored
157	The clearance subject's eligibility and suitability to hold a Baseline, Negative Vetting 1, Negative Vetting 2 or Positive Vetting security clearance is assessed by resolving any doubt in the national interest.	PER	19. Personnel Security Vetting Process	Authorised Vetting Agency	31/10/2024	Retain	Performance	Mandatory - only for AVA	Scored
158	Concerns that are identified during the vetting or security clearance suitability assessment process, that are not sufficient to deny a security clearance and where the related risks can be managed through conditions attached to the security clearance, the Authorised Vetting Agency must: • identify the clearance conditions • provide the sponsoring entity with information about the concerns to inform a risk assessment • only issue a conditional security clearance if the Accountable Authority and the clearance subject accept the clearance conditions. The Accountable Authority may delegate this decision to the Chief Security Officer, however the Chief Security Officer is required to notify the Accountable Authority of the clearance conditions.	PER	19. Personnel Security Vetting Process	Authorised Vetting Agency	31/10/2024	Retain	Performance	Mandatory - only for AVA	Scored
159	The Authorised Vetting Agency provides the sponsoring entity any relevant information of concern, when advising them of the outcome of the security vetting process, to inform the sponsoring entity's risk assessment.	PER	19. Personnel Security Vetting Process	Authorised Vetting Agency	31/10/2024	Retain	Performance	Mandatory - only for AVA	Scored
160	The Authorised Vetting Agency applies the rules of procedural fairness to security clearance decisions that are adverse to a clearance subject, including decisions to deny a security clearance (including grant lower level) or grant a conditional security clearance, without compromising the national interest. *Note: Separate arrangements ensure procedural fairness and national security are preserved where denial of a clearance is based on an ASIO security clearance suitability assessment.*	PER	19. Personnel Security Vetting Process	Authorised Vetting Agency	31/10/2024	Retain	Performance	Mandatory - only for AVA	Scored
161	The Authorised Vetting Agency reviews the conditions of conditional security clearances annually.	PER	21. Maintenance and Ongoing Assessment	Authorised Vetting Agency	31/10/2024	Retain	Performance	Mandatory - only for AVA	Scored
162	The Authorised Vetting Agency reviews the clearance holder's eligibility and suitability to hold a security clearance, where concerns are identified (review for cause).	PER	21. Maintenance and Ongoing Assessment	Authorised Vetting Agency	31/10/2024	Retain	Performance	Mandatory - only for AVA	Scored
163	The Authorised TOP SECRET-Privileged Access Vetting Agency implements the TOP SECRET-Privileged Access Standard in relation to the ongoing assessment and management of personnel with TOP SECRET-Privileged Access security clearances.	PER	21. Maintenance and Ongoing Assessment	Authorised Vetting Agency	31/10/2024	Retain	Performance	Mandatory - only for AVA	Scored
164	The Sponsoring Entity actively assesses, monitors and manages the ongoing suitability of personnel.	PER	21. Maintenance and Ongoing Assessment	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
165	The Sponsoring Entity monitors and manages compliance with any conditional security clearance requirements and reports any non-compliance to the Authorised Vetting Agency.	PER	21. Maintenance and Ongoing Assessment	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
166	The Sponsoring Entity monitors and manages compliance with security clearance maintenance obligations for the clearance holders they sponsor.	PER	21. Maintenance and Ongoing Assessment	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
167	The Sponsoring Entity shares relevant information of concern, where appropriate.	PER	21. Maintenance and Ongoing Assessment	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
168	The Sponsoring Entity conducts an annual security check with all security cleared personnel.	PER	21. Maintenance and Ongoing Assessment	All entities	31/10/2024	Retain	Performance	Mandatory	Scored

169	The Sponsoring Entity reviews eligibility waivers at least annually, before revalidation of a security clearance, and prior to any proposed position transfer.	PER	21. Maintenance and Ongoing Assessment	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
170	The Sponsoring Entity monitors, assesses and manages personnel with TOP SECRET-Privileged access security clearances in accordance with the TOP SECRET-Privileged Access Standard.	PER	21. Maintenance and Ongoing Assessment	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
171	The Authorised Vetting Agency reassesses a clearance holder's eligibility and suitability to hold a security clearance by revalidating minimum personnel security checks for a security clearance.	PER	21. Maintenance and Ongoing Assessment	Authorised Vetting Agency	31/10/2024	Retain	Performance	Mandatory - only for AVA	Scored
172	The Authorised Vetting Agency reassesses a clearance holder's eligibility and suitability to hold a Baseline, Negative Vetting 1, Negative Vetting 2 or Positive Vetting security clearance by considering their integrity in accordance with the Australian Government Personnel Security Adjudicative Standard.	PER	21. Maintenance and Ongoing Assessment	Authorised Vetting Agency	31/10/2024	Retain	Performance	Mandatory - only for AVA	Scored
173	The TOP SECRET-Privileged Access Vetting Authority reassesses a clearance holder's eligibility and suitability to hold a TOP SECRET-Privileged Access security clearance by assessing their trustworthiness in accordance with the TOP SECRET-Privileged Access Standard.	PER	21. Maintenance and Ongoing Assessment	Authorised Vetting Agency	31/10/2024	Retain	Performance	Mandatory - only for AVA	Scored
174	The Authorised Vetting Agency reassesses a clearance holder's eligibility and suitability to hold a security clearance by resolving any doubt in the national interest.	PER	21. Maintenance and Ongoing Assessment	Authorised Vetting Agency	31/10/2024	Retain	Performance	Mandatory - only for AVA	Scored
175	The Authorised Vetting Agency commences the security clearance revalidation process in sufficient time to complete the revalidation before the due date so that the security clearance does not lapse.	PER	21. Maintenance and Ongoing Assessment	Authorised Vetting Agency	31/10/2024	Retain	Performance	Mandatory - only for AVA	Scored
176	The Authorised Vetting Agency shares information of concern about security clearance holders with the Sponsoring Entity so they can decide whether to suspend or limit the clearance holder's access to Australian Government classified information, resources or activities until the concerns are resolved.	PER	21. Maintenance and Ongoing Assessment	Authorised Vetting Agency	31/10/2024	Retain	Performance	Mandatory - only for AVA	Scored
177	The Sponsoring Entity shares relevant information of security concern, where appropriate with the Authorised Vetting Agency.	PER	21. Maintenance and Ongoing Assessment	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
178	The Authorised Vetting Agency shares information of security concern about security clearance holders with the Sponsoring Entity.	PER	21. Maintenance and Ongoing Assessment	Authorised Vetting Agency	31/10/2024	Retain	Performance	Mandatory - only for AVA	Scored
179	The Authorised Vetting Agency assesses and responds to information of security concern about security clearance holders, including reports from Sponsoring Entities.	PER	21. Maintenance and Ongoing Assessment	Authorised Vetting Agency	31/10/2024	Retain	Performance	Mandatory - only for AVA	Scored
180	Negative Vetting 2 and higher clearance holders receive appropriate departmental travel briefings when undertaking international personal and work travel.	PER	21. Maintenance and Ongoing Assessment	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
181	The Chief Security Officer, Chief Information Security Officer (or other relevant security practitioner) is advised prior to separation or transfer of any proposed cessation of employment resulting from misconduct or other adverse reasons.	PER	22. Separation	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
182	Separating personnel are informed of any ongoing security obligations under the Commonwealth Criminal Code and other relevant legislation and those holding a security clearance or access security classified information are debriefed prior to separation from the entity.	PER	22. Separation	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
183	Separating personnel transferring to another Australian Government entity, the entity, when requested, provides the receiving entity with relevant security information, including the outcome of pre-employment screening checks and any periodic employment suitability checks.	PER	22. Separation	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
184	Separating personnel transferring to another Australian Government entity, the entity reports any security concerns (as defined in the Australian Security Intelligence Organisation Act 1979) to the Australian Security Intelligence Organisation.	PER	22. Separation	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
185	A risk assessment is completed to identify any security implications in situations where it is not possible to undertake the required separation procedures.	PER	22. Separation	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
186	Separating personnel have their access to Australian Government resources withdrawn upon separation or transfer from the entity, including information, technology systems, and resources.	PER	22. Separation	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
187	The Sponsoring Entity advises the relevant Authorised Vetting Agency of the separation of a clearance holder, including any relevant circumstances (e.g. termination for cause) and any details, if known, of another entity or contracted service provider the clearance holder is transferring to, along with any identified risks or security concerns associated with the separation.	PER	22. Separation	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
188	The Authorised Vetting Agency manages and records changes in the security clearance status of separating personnel, including a change of Sponsoring Entity, and transfer personal security files where a clearance subject transfers to an entity covered by a different Authorised Vetting Agency, to the extent that their enabling legislation allows.	PER	22. Separation	All entities	31/10/2024	Retain	Performance	Mandatory - only for AVA	Scored
189	Protective security is integrated in the process of planning, selecting, designing and modifying entity facilities for the protection of people, information and resources.	PHYS	23. Physical Security Lifecycle	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
190	A facility security plan is developed for new facilities, facilities under construction or major refurbishments of existing facilities.	PHYS	23. Physical Security Lifecycle	All entities	31/08/2024	Retain	Performance	Mandatory	Scored
191	Decisions on entity facility locations are informed by considering the site selection factors for Australian Government facilities.	PHYS	23. Physical Security Lifecycle	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
192	When designing or modifying facilities, the entity secures and controls access to facilities to meet the highest risk level to entity resources in accordance with Security Zone restricted access definitions.	PHYS	23. Physical Security Lifecycle	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
193	Facilities are constructed in accordance the applicable ASIO Technical Notes to protect against the highest risk level in accordance with the entity security risk assessment in areas: • accessed by the public and authorised personnel, and • where physical resources and technical assets, other than security classified resources and technology, are stored.	PHYS	23. Physical Security Lifecycle	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
194	Facilities for Security Zones Two to Five that process, store or communicate security classified information and resources are constructed in accordance with the applicable sections of ASIO Technical Note 1/15 – Physical Security Zones, and ASIO Technical Note 5/12 – Physical Security Zones (TOP SECRET) areas.	PHYS	23. Physical Security Lifecycle	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
195	Entity facilities are operated and maintained in accordance with Security Zones and Physical Security Measures and Controls.	PHYS	23. Physical Security Lifecycle	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
196	Security Zones One to Four are certified by the Certification Authority in accordance with the PSPF and applicable ASIO Technical Notes before they are used operationally.	PHYS	24. Security Zones	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
197	Security Zone Five areas that contain TOP SECRET security classified information or aggregated information where the compromise of confidentiality, loss of integrity or unavailability of that information may have a catastrophic business impact level, are certified by ASIO-T4 before they are used operationally.	PHYS	24. Security Zones	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
198	Security Zones One to Five are accredited by the Accreditation Authority before they are used operationally, on the basis that the required security controls are certified and the entity determines and accepts the residual risks.	PHYS	24. Security Zones	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
199	Sensitive Compartmented Information Facility areas used to secure and access TOP SECRET systems and security classified compartmented information are accredited by the Australian Signals Directorate before they are used operationally.	PHYS	24. Security Zones	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
200	Physical security measures are implemented to minimise or remove the risk of information and physical asset resources being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.	PHYS	25. Physical Security Measures and Controls	All entities	31/08/2024	Retain	Performance	Mandatory	Scored
201	Physical security measures are implemented to protect entity resources, commensurate with the assessed business impact level of their compromise, loss or damage.	PHYS	25. Physical Security Measures and Controls	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
202	Physical security measures are implemented to minimise or remove the risk of harm to people.	PHYS	25. Physical Security Measures and Controls	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
203	The appropriate container, safe, vault, cabinet, secure room or strong rooms is used to protect entity information and resources based on the applicable Security Zone and business impact level of the compromise, loss or damage to information or physical resources.	PHYS	25. Physical Security Measures and Controls	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
204	Perimeter doors and hardware in areas that process, store or communicate security classified information or resources are constructed and secured in accordance with the physical security measures and controls for perimeter doors and hardware.	PHYS	25. Physical Security Measures and Controls	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
205	Access by authorised personnel, vehicles and equipment to Security Zones One to Five is controlled in accordance with the physical security measures and controls for access control for authorised personnel.	PHYS	25. Physical Security Measures and Controls	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
206	Access by visitors to Security Zones One to Five is controlled in accordance with the physical security measures and controls for access control for visitors.	PHYS	25. Physical Security Measures and Controls	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
207	The Accountable Authority or Chief Security Officer approves ongoing (or regular) access to entity facilities for people who are not directly engaged by the entity or covered by the terms of a contract or agreement, on the basis that the person: • has the required security clearance level for the Security Zone/s, and • a business need supported by a business case and security risk assessment, which is reassessed at least every two years.	PHYS	25. Physical Security Measures and Controls	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
208	Unauthorised access to Security Zones One to Five is controlled in accordance with the physical security measures and controls for security alarm systems.	PHYS	25. Physical Security Measures and Controls	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
209	Security guard arrangements in Security Zones One to Five are established in accordance with the physical security measures and controls for security guards.	PHYS	25. Physical Security Measures and Controls	All entities	31/10/2024	Retain	Performance	Mandatory	Scored
210	Technical surveillance countermeasures for Security Zones One to Five are established in accordance with the physical security measures and controls for technical surveillance countermeasures.	PHYS	25. Physical Security Measures and Controls	All entities	31/10/2024	Retain	Performance	Mandatory	Scored

PSPF Recommended Approach	Domain	Section	Applicability (All, Dept of State, Security Service Provider Entity, Technical Authority Entity, Authorised Vetting Agency)
Implement appropriate oversight arrangements, including appointing an executive to coordinate security services to supported entities.	GOV	1.1.1 Current Departments of State	Department of State (DOS)
Sustain capability to provide timely and accurate security advice and services.	GOV	1.1.1 Current Departments of State	Department of State (DOS)
Maintain regular contact with the entities they support to increase awareness of the lead security entity's role and capabilities.	GOV	1.1.1 Current Departments of State	Department of State (DOS)
Ensure the technical advice and guidance to support government entities to achieve and maintain and acceptable level of protective security is provided in a timely manner and through appropriate channels.	GOV	1.3.1 Current Technical Authority Entities	Technical Advisory Entities (TAE)
Ensure technical standards, policy guidance and manuals remain aligned with the annual PSPF release.	GOV	1.3.1 Current Technical Authority Entities	Technical Advisory Entities (TAE)
Establish clear responsibilities (agreed by all parties) including who will take lead control, and when.	GOV	1.4 Shared Service Provider Entities	Shared Service Provider Entities (SSPE)
Establish arrangements for seeking technical or specialist advice to inform decisions about the shared arrangements.	GOV	1.4 Shared Service Provider Entities	Shared Service Provider Entities (SSPE)
Establish escalation responsibilities (to whom and when), particularly if there are multiple ministers or governing bodies involved.	GOV	1.4 Shared Service Provider Entities	Shared Service Provider Entities (SSPE)
Establish communication channels to maintain the flow of information between relevant parties (e.g. leadership, staff, contractors, building owners, in-house service providers) during an event or security incident.	GOV	1.4 Shared Service Provider Entities	Shared Service Provider Entities (SSPE)
Apply a consistent approach, particularly for services to co-located entities.	GOV	1.4 Shared Service Provider Entities	Shared Service Provider Entities (SSPE)
Schedule periodic reviews to consider the effectiveness of these arrangements and make procedural adjustments where necessary.	GOV	1.4 Shared Service Provider Entities	Shared Service Provider Entities (SSPE)
The CSO is an appropriate level of seniority in the entity to achieve the protective security oversight functions, foster a positive security culture and drive improvements in protective security practice.	GOV	2.2.1 Chief Security Officer Responsibilities	All entities
The CSO has sufficient experience or be trained to perform the required security leadership and oversight functions.	GOV	2.2.1 Chief Security Officer Responsibilities	All entities
The CSO secures sufficient funding and resources to ensure the protection of the entity's people, information and resources.	GOV	2.2.1 Chief Security Officer Responsibilities	All entities
The CSO chairs the entity's security governance committee (if established), or otherwise holds membership on relevant internal committees.	GOV	2.2.1 Chief Security Officer Responsibilities	All entities
The CISO is an appropriate level of seniority in the entity to perform the cyber security leadership functions of the role and make informed cyber security decisions for the entity.	GOV	2.3.1 Chief Information Security Officer Responsibilities	All entities
The CISO reports to the CSO, or otherwise works closely with the CSO to ensure a holistic approach to security is maintained	GOV	2.3.1 Chief Information Security Officer Responsibilities	All entities
The CISO is an appropriate level of seniority in the entity to achieve the cyber security functions.	GOV	2.3.1 Chief Information Security Officer Responsibilities	All entities
The CISO holds a security clearance at the level commensurate with the entity's data holdings (with Negative Vetting 1 being the minimum as per PSPF Requirement 0012.	GOV	2.3.1 Chief Information Security Officer Responsibilities	All entities
The CISO holds membership on the security governance committee, if established within the entity.	GOV	2.3.1 Chief Information Security Officer Responsibilities	All entities
Cyber security practitioners report to a single senior officer, preferable the CISO, particular in larger entities, complex entities, or entities that carry high-risk and require multiple cyber security practitioners to manage cyber security-related functions.	GOV	2.3.1 Chief Information Security Officer Responsibilities	All entities
Sufficient security practitioner positions are in place to perform security functions to support the continuous delivery of the entity's business operations.	GOV	2.5.2.1. Distribution of PSPF-Related Information	All entities
Each security practitioner position has clearly defined responsibilities with sufficient authority to perform those responsibilities and achieve the entity's security objectives.	GOV	2.5.2.1. Distribution of PSPF-Related Information	All entities
Security practitioners work together to ensure consistent approach to protective security, maintain appropriate visibility over entity security operations and decisions, and have regular access to the entity's CSO and/or CISO.	GOV	2.5.2.1. Distribution of PSPF-Related Information	All entities
Security practitioners attend relevant industry conferences, training and events to ensure their knowledge and skills keep pace with change.	GOV	2.5.2.1. Distribution of PSPF-Related Information	All entities
The CSO is the Chair of the Security Governance Committee (if established in the entity).	GOV	2.5.2.1. Distribution of PSPF-Related Information	All entities
The CISO is a member of the Security Governance Committee (if established in the entity).	GOV	2.5.2.1. Distribution of PSPF-Related Information	All entities
The Security Governance Committee meets on a regular basis to monitor all areas of security and support informed decisions on security arrangements for the entity, and provides the Accountable Authority with regular reports on the status of the entity's security posture and compliance position.	GOV	2.5.2.1. Distribution of PSPF-Related Information	All entities
The generic security email address takes the form **security@[entityname].gov.au** or **pspf@[entityname].gov.au**	GOV	2.5.2.1. Distribution of PSPF-Related Information	All entities
The generic security email is monitored to ensure the flow of security-related information to the Accountable Authority, CSO, CISO, security practitioners, security governance committee members and other relevant areas in the entity.	GOV	2.5.2.1. Distribution of PSPF-Related Information	All entities
The entity advises the Department of Home Affairs of any changes in CSO, CISO or generic security email address to PSPF@homeaffairs.gov.au	GOV	2.5.2.1. Distribution of PSPF-Related Information	All entities
A single security plan, or an overarching security plan where impracticable due to the entity's size or complexity, is approved by the Accountable Authority.	GOV	3.1.1 Security Plan Responsibilities	All entities
Supporting security plans (where required) are approved by the CSO or CISO (for cyber security plans), or their delegate.	GOV	3.1.1 Security Plan Responsibilities	All entities
Entities liaise with other internal corporate areas (for example human resources, business continuity, property and procurement) to ensure an embedded approach, to understand the strategic direction of these areas and to identify any potential impacts on security planning.	GOV	3.1.1 Security Plan Responsibilities	All entities
Security plans are comprehensive and span all areas of protective security	GOV	3.1.3 Developing a Security Plan	All entities
Security plans are informed by expert or technical advice (where required).	GOV	3.1.3 Developing a Security Plan	All entities
When setting goals, consider the historical experience and knowledge results from previous performance indicators and past compliance with the PSPF.	GOV	3.1.3.1 Element: Security Goals and Objectives	All entities
Entities assess their existing protective security arrangements and procedures to identify areas for improvement. This could be areas of exposure, vulnerability or 'target attractiveness'. Target attractiveness is the value of an entity or its components to an adversary when viewed as a target.	GOV	3.1.3.1 Element: Security Goals and Objectives	All entities
Reviewing protective security arrangements should also consider the entity's compliance with implementing PSPF requirements.	GOV	3.1.3.1 Element: Security Goals and Objectives	All entities
Adopt a security risk management approach that is compatible with security requirements, the entity's risk profile and aligns with the relevant risk management standards, such as: - Department of Finance's Commonwealth Risk Management Policy - Australian Standards AS/NZS ISO 31000 Risk Management – Guidelines and HB 167 – Security Risk Management.	GOV	3.1.3.2. Element: Security Risk Environment	All entities
Security arrangements support the entity's business objectives by identifying and managing risks that could adversely affect achieving those objectives.	GOV	3.1.3.13. Element: Review	All entities
The entity's historical security experience, security performance and past compliance with the PSPF is considered when setting security goals and objectives.	GOV	3.1.3.13. Element: Review	All entities
The entity's areas of exposure, vulnerability or 'target attractiveness' (the value of an entity or its components to an adversary when viewed as a target) is considered when setting security goals and objectives.	GOV	3.1.3.13. Element: Review	All entities
Entities review their security plan when there are significant shifts in the entity's risk or operating environment.	GOV	3.1.4 Security Plan Review	All entities
Entities develop security procedures in conjunction with other security and risk planning and update these procedures when significant changes in the risk environment occur.	GOV	3.2 Security Practices and Procedures	All entities
Establish any entity-specific practices or procedures that are required for the entity's unique operating environment or operational needs.	GOV	3.2 Security Practices and Procedures	All entities
Entities put in place measures to monitor the effectiveness of procedures and security performance and update annual security awareness training with relevant messaging.	GOV	3.2 Security Practices and Procedures	All entities
Develop their security maturity monitoring plan as part of their overarching security plan. This includes: - using security maturity indicators as detailed in the PSPF Risk-Based Compliance Reporting Model - setting goals and objectives and identifying the impact on security of any goals and objectives detailed in the entity security plan - developing methodologies to manage the collection, measurement and analysis of data in relation to the entity's security maturity indicators - determining the frequency of security monitoring advice to be given to the Accountable Authority, CSO, audit committee and relevant security governance committee (if established in the entity) - setting pre-determined levels of change in security maturity metrics that trigger escalation to the Accountable Authority, CSO, audit committee and relevant security governance committees, and - where applicable, identifying the responsible area and timeframes to: -manage implementation of PSPF requirements -implement strategies that achieve improvements in security culture.	GOV	3.3 Continuous Monitoring and Improvement	All entities
CSO considers the entity's risk and current threat environment, goals and objectives of the entity's security plan, and any identified inadequacies in previous methods of training or consistent failure to understand content, particularly when systemic or repeated security incidents indicate potential vulnerabilities in awareness training.	GOV	3.5.1 Effective Security Awareness Training	All entities
CSO decides the most appropriate delivery method for security awareness training to ensure consistent delivery within their entity and others the entity provides training to as part of a lead security arrangement.	GOV	3.5.1 Effective Security Awareness Training	All entities
Security awareness training is tailored to your entity's risks, security practices and procedures and functions.	GOV	3.5.1 Effective Security Awareness Training	All entities
Security awareness training is practical and promotes personal responsibility for protective security, regardless of the role or level of seniority in the entity.	GOV	3.5.1 Effective Security Awareness Training	All entities
Security awareness training uses a mixture of delivery methods and follows principles of adult education.	GOV	3.5.1 Effective Security Awareness Training	All entities
If used, outsourced training providers of security awareness training have sufficient knowledge of the PSPF and expertise in delivering adult education.	GOV	3.5.1 Effective Security Awareness Training	All entities

Security drills and exercises are regularly carried out to gauge people's knowledge and the effectiveness of the entity's security awareness training.	GOV	3.5.7 Security Awareness Refresher Training	All entities
Security awareness training is updated annually to reflect the annual PSPF release, any changes in the entity's operations or security arrangements, and to address inadequacies in previous training methods.	GOV	3.5.7 Security Awareness Refresher Training	All entities
Where security investigation functions are shared across entity work areas or with an outsourced service provider, the CSO, CISO (or another delegated SES officer) should maintain oversight of the investigation and establish mechanisms to monitor the investigation and ensure communication of issues, findings and decisions to all relevant parties.	GOV	3.6.3 Coordination of Cyber Security Incidents	All entities
Simple channel for personnel (including contractors and personnel travelling or working remotely) to report security incidents, or suspected incidents, is established to promote timely reporting.	GOV	3.6.3 Coordination of Cyber Security Incidents	All entities
Security awareness training covers reporting security incidents and provides practical examples and potential consequences.	GOV	3.6.3 Coordination of Cyber Security Incidents	All entities
Additional identification and monitoring detection methods are established to supplement reporting of security incidents by personnel.	GOV	3.6.3.2. Report and Remediate Security Incidents	All entities
Establish internal reporting and recovery plans.	GOV	3.6.3.2. Report and Remediate Security Incidents	All entities
Record the details of each reported security incident, including: - time, date and location of security incident, including how the incident was detected - type of official resources involved - description of the circumstances of the incident, including any personnel or locations involved - nature or intent of the incident, e.g. deliberate or accidental - assessment of the degree of compromise or harm - whether it is an isolated incident or part of a broader reoccurring issue, and a - summary of immediate action (including containment or eradication) and any long-term action taken (including post-incident activities).	GOV	3.6.3.3. Record Security Incidents	All entities
CSO and CISO (for cyber incidents) maintains oversight of recorded security incidents and regularly analyses them to identify trends and systemic issues.	GOV	3.6.3.3. Record Security Incidents	All entities
Complete a post incident review of significant security incidents to identify areas for improvement and where required, update training, security incident management plans and security exercises,	GOV	3.6.3.3. Record Security Incidents	All entities
Identify, document and share learnings internally (i.e. with and between the Accountable Authority, security practitioners and security governance committee) and externally, where appropriate (i.e. with co-located entities, entities with similar risk profiles or through whole-of-government arrangements).	GOV	3.6.3.4. Learn from Security Incidents	All entities
A post incident analysis is conducted after each significant security incident to identify areas for improvement and lessons learnt to inform handling of future incidents.	GOV	3.6.3.4. Learn from Security Incidents	All entities
Information gathered from security incidents informs is used by CSO/CISO to determine the adequacy of protective security practices, measure security culture, highlight vulnerabilities in security awareness training and inform security improvement activities.	GOV	3.6.3.4. Learn from Security Incidents	All entities
Where security investigation functions are shared across entity work areas or with an outsourced service provider, the CSO, CISO (or another delegated SES officer) maintain oversight of the investigation and establish mechanisms to monitor the investigation and ensure communication of issues, findings and decisions to all relevant parties.	GOV	3.7 Security Investigations	All entities
When conducting a security investigation, evidence is gathered in a manner that ensures the integrity of the evidence is maintained.	GOV	3.7 Security Investigations	All entities
CSO approve the terms of reference, objectives and limits for all security investigations.	GOV	3.7.2.2. Develop an Investigation Plan	All entities
CSO seeks regular progress reports on active investigations.	GOV	3.7.2.2. Develop an Investigation Plan	All entities
A separate and complete file is maintained by the investigator for each investigation that documents dates and times of all discussions, phone calls and interviews, and captures decisions and conclusions made during the course of the investigation.	GOV	3.7.2.3. Gather, Record and Store Evidence	All entities
This file, and any physical evidence, is stored securely to prevent unauthorised access, damage or alteration, and to maintain confidentiality and continuity of the evidence. It is important that the record includes the handling of physical evidence and any tampering with the file or physical evidence.	GOV	3.7.2.3. Gather, Record and Store Evidence	All entities
Accountable Authority documents the entity's protections to reduce, treat or mitigate risks, including the defined benchmarks against which the success of implemented risk mitigations are measured.	RISK	5.1 Security Risk Tolerance	All entities
Consider where security risks intersect with other risks including fraud, privacy and business continuity.	RISK	5.2.1 Security Risk	All entities
Treat risk holistically across the entity's operations and identify opportunities to treat multiple risks with one mitigation control.	RISK	5.2.1 Security Risk	All entities
Consider where security risks intersect with other risks including fraud, privacy and business continuity.	RISK	5.2.2 Shared Security Risk	All entities
Security risks arising from co-tenancy or shared facilities are addressed by applying protective security.	RISK	5.2.2 Shared Security Risk	All entities
Security risks associated with a particular location (e.g. physical boundaries, crowded public space, government precinct) where there is no identifiable other party to share the assessment and management of the risk, the entity mitigates the risk to the extent it is able to within its operations	RISK	5.2.2 Shared Security Risk	All entities
When selecting treatment, the entity balances the cost and effort of implementing the treatment with the expected benefits and ensure the treatment is proportional to the determined risk rating level.	RISK	5.2.5 Security Risk Treatment	All entities
Adopt a risk-rating-matrix approach for determining the levels of risk.	RISK	5.2.5 Security Risk Treatment	All entities
Consult experienced subject matter experts as part of the risk assessment process, when warranted by the scale, scope and nature of the security risks involved in the procurement.	RISK	6.1.1 Procurement of Outsourced Services	All entities
Identify who is accountable for each security treatment or control in the contract.	RISK	6.1.2 Ongoing Management of Security in Contracts	All entities
Evaluate compliance with contract conditions by performing ongoing assessments (such as regular inspection of premises used to store Australian Government information or resources, or an ongoing accreditation program).	RISK	6.1.2.1. Monitor and Review Contracts	All entities
Identify a contract manager who is responsible for monitoring and reviewing risk for each contract can assist in this process.	RISK	6.1.2.1. Monitor and Review Contracts	All entities
Complete a review where elevated risks are identified.	RISK	6.1.3.5. Monitor and Review FOCI Risks	All entities
Establish contract conditions that require the third-party service provider or vendor to notify the entity of any changes in ownership or control.	RISK	6.1.3.5. Monitor and Review FOCI Risks	All entities
Consider who is best placed to undertake the review in the entity, for example the Chief Information Security Officer may undertake the review in consultation with the procurement team and provide a report to the entity's audit and risk committee or security governance committee.	RISK	6.1.3.5. Monitor and Review FOCI Risks	All entities
Provide personnel with clearly defined points-of-contact for them to report actual or suspected insider threat acts, or seek advice on concerns relating to insider threat.	RISK	7.3.1 Countering the Insider Threat	All entities
Senior leaders are appointed to act as 'champions' of the entity's insider threat program.	RISK	7.3.1 Countering the Insider Threat	All entities
Consider alternative mitigation strategies during periods of exceptional circumstances to maintain appropriate protection of the impacted PSPF requirements.	RISK	8.1 Exceptional Circumstances	All entities
Develop an entity procedure for noting when the originator has approved the reclassification or declassification of information.	INFO	9.1.1 Sanitisation, Reclassification or Declassification	All entities
Establish procedures so that information is automatically declassified if the originator sets a specific date or event for declassification based on an assessment of the period in which the information might cause damage; otherwise when the open access period under the Archives Act 1983.	INFO	9.1.1 Sanitisation, Reclassification or Declassification	All entities
Establish procedures to encourage regular reviews of classified information for continuing sensitivity (i.e. if the compromise of the information would still cause damage) using the impact based classification assessment. - For example, these reviews could be done after a project is completed or when a file is withdrawn from (or returned to) use. Information is declassified or reclassified to a lower classification when a reassessment of its Business Impact Level indicates it no longer meets the original Business Impact Level to which its classification applies.	INFO	9.1.1 Sanitisation, Reclassification or Declassification	All entities
Ensure the use or presence of privately-owned mobile devices do not present an unacceptable security risk.	INFO	9.3 Minimum Protections and Handling Requirements	All entities
Develop entity-specific protections for security classified information where a higher level of protection is required to meet business needs or the entity's security risk environment.	INFO	9.3 Minimum Protections and Handling Requirements	All entities
Develop procedures for assessing the risks of medical devices to support staff working in Zones 4 and 5.	INFO	9.3 Minimum Protections and Handling Requirements	All entities
Mobile devices are not stored in locations where meetings or discussions of a higher classification are held unless the device is protected by a visual and audio suppression container.	INFO	9.3.2 Carry Security Classified Information	All entities
Establish sound record keeping procedures for sharing with international stakeholders that demonstrates the appropriateness of information sharing.	INFO	12.3.1 Provisions for International Information Sharing	All entities
Review the relevant international agreement or arrangement to identify additional obligations or protections that may differ from the PSPF requirements.	INFO	12.3.2 International Stakeholder Information and Resources	All entities
Report security incidents to the originating foreign government as soon as possible.	INFO	12.3.3.1. Ad Hoc Process for Sharing with Foreign Governments	All entities
Apply the TSRMP to all technology assets and services within an entity's technology estate.	TECH	13.2.2.2. Technology Security Risk Management Plan	All entities
Annual reporting by an entity's system owners to the entity's Authorised Officer on the security status of their technology systems can assist in maintaining awareness of the security posture of the technology systems within the entity.	TECH	13.3.2 System Owners	All entities
Implement a mitigation strategy that first implements for high risk users and computers with access to important (security classified or high-availability) data for internet-facing services and systems before implementing more broadly.	TECH	14.2 Essential Eight Strategies	All entities
Monitor relevant sources for information about new security vulnerabilities and associated patches for applications and operating systems.	TECH	14.2.1 Patch Applications	All entities
Implement a centralised and managed approach to patching operating systems and applications (where possible), including by regularly scanning for missing patches.	TECH	14.2.1 Patch Applications	All entities
Confirm that patches have been installed, applied successfully and remain in place.	TECH	14.2.1 Patch Applications	All entities
Implement an application control solution to mitigate malicious macros running unapproved applications.	TECH	14.2.6 Restrict Microsoft Office Macro Settings	All entities
Prevent users from changing macro security settings within Microsoft Office applications.	TECH	14.2.6 Restrict Microsoft Office Macro Settings	All entities

Entities should be aware that the use of an upstream PDNS resolver service could impair security features, such as web proxies, mail relays, sandbox and malware analysis platforms, and SIEM tools, and should assess and evaluate to ensure their security platforms are functional correctly.	TECH	15.1 Whole of Government Cyber Security Service	All entities
Entities are strongly recommended to use the ASD's Anatomy of a Cloud Assessment and Authorisation for guidance when performing a security assessment to determine the suitability of a particular cloud service provider and its cloud services.	TECH	15.2.1 Australian Government Hosting Certification Framework	All entities
Where an entity intends to grant temporary access to security classified information from another entity or third party, they should consult the other entity or party and obtain agreement for temporary access to their security classified information.	PER	17.1 Temporary Access to Resources	All entities
Prevent an individual from holding concurrent eligibility waivers (citizenship and checkable background).	PER	17.1 Temporary Access to Resources	All entities
Obtain a confidentiality or non-disclosure agreement to protect security classified information.	PER	17.1 Temporary Access to Resources	All entities
Strengthen user identification, authentication and authorisation for higher-risk users by implementing additional personnel and physical security controls strategies.	PER	17.2.2.1. User Identification, Authentication and Authorisation	All entities
Establish procedures that take into consideration country-specific travel advice and guidance.	PER	17.3 Remote Access to Resources	All entities
Consult DFAT for practical advice, including on the availability of transfer and storage options using resources available through Australian Government embassies, high commissions and consulates.	PER	17.3 Remote Access to Resources	All entities
Establish procedures that take into consideration country-specific travel advice and guidance.	PER	17.3.2 Working Remotely Outside of Australia (International)	All entities
Treat any non-Australian Government facilities as Zone One areas for the storage and/or use of security classified information and resources unless the entity has full control over the work space occupied by their personnel in commercial and client facilities and has confirmed appropriate physical and procedural security measures are in place for a high level zone.	PER	17.3.2.2. Working Outside of an Australian Government International Entity Facility, Mission or Post	All entities
Authorised Vetting Agencies comprehensively document information obtained through a digital footprint check because of the changing nature of online information.	PER	19.1.1 Informed Consent	Authorised Vetting Agencies (AVA)
Information should have a relevant bearing on a clearance subject's suitability to hold a security clearance, including screenshots and direct links where possible.	PER	19.1.1 Informed Consent	All entities
When determining suitability, Authorised Vetting Agencies should establish and use a process of structured professional judgement to come to an overall determination based on all the available information for a clearance subject.	PER	19.2 Personnel Security Adjudicative Standard	All entities
Authorised Vetting Agencies should use a questionnaire to gather initial background assessment information from clearance subjects.	PER	19.3.3 Background Assessment Check	Authorised Vetting Agencies (AVA)
Authorised Vetting Agencies should document all attempts to satisfy the background checking requirement. - This includes alternative measures undertaken, any identified risks and how identified risks were mitigated (if mitigation is possible). - This information will inform any review process in the event of an adverse decision or inform the Sponsoring Entity's risk management in the event that a clearance is granted subject to waiver.	PER	19.3.3 Background Assessment Check	Authorised Vetting Agencies (AVA)
Authorised Vetting Agencies should contact previous government employers to determine if the clearance subject has previously been found to have breached the code of conduct, if there are current investigations into a possible breach of the code of conduct or if there are any integrity issues or identified concerns.	PER	19.3.5 Referee Checks	Authorised Vetting Agencies (AVA)
Authorised Vetting Agencies should corroborate and verify the integrity of the information if the digital footprint check identifies information of security concern.	PER	19.3.6.2. Minimum Digital Footprint Checks	Authorised Vetting Agencies (AVA)
Issues in attributing information to the clearance subject should be raised with the clearance subject to provide them with an opportunity to clarify or provide further information.	PER	19.3.6.2. Minimum Digital Footprint Checks	All entities
Authorised Vetting Agencies should account for missing or inaccurate information and the possibility of a clearance subject (or third party) sanitising or obfuscating their digital footprint to create a misleading impression.	PER	19.3.6.2. Minimum Digital Footprint Checks	Authorised Vetting Agencies (AVA)
Discrepant information, or where it is apparent information obtained through a digital footprint check has been omitted by the clearance subject in other vetting checks (e.g. close associates of foreign nationality, significant life events and international travel or employment), should be resolved by the Authorised Vetting Agency.	PER	19.3.6.2. Minimum Digital Footprint Checks	All entities
The Authorised Vetting Agency should request a bankruptcy check in writing through the Insolvency and Trustee Service Australia, where a clearance subject has indicated that they have been bankrupt or insolvent.	PER	19.3.8 Financial History Assessment Check	Authorised Vetting Agencies (AVA)
Vetting analysts should undertake specialist training or seek specialist advice before undertaking complex financial analysis.	PER	19.3.9 Financial Statement Check	All entities
Authorised Vetting Agencies should negotiate with ASIO on a case-by-case basis where operational needs require the ASIO security clearance suitability assessment to be conducted concurrently with other checks.	PER	19.3.12 ASIO Security Clearance Suitability Assessment Check	Authorised Vetting Agencies (AVA)
Face-to-face, video or telephone interviews should address all factor areas in the Australian Government Personnel Security Adjudicative Standard and any specific areas of concern.	PER	19.3.13 Security Interview Check	All entities
Authorised Vetting Agency should establish effective procedures to document and share adverse information with Sponsoring Entities. This includes procedures to identify mitigation activities that Sponsoring Entities could undertake to manage risks in relation to the clearance subject's ongoing suitability.	PER	19.6 Sharing Information of Concern	Authorised Vetting Agencies (AVA)
Authorised Vetting Agency should consider whether an outsourced vetting service provider is able to manage procedural fairness issues involving outsourced vetting services.	PER	19.7 Procedural Fairness	Authorised Vetting Agencies (AVA)
An entities' procedures for assessing and managing the ongoing suitability of personnel include periodic employment suitability checks, as well as mechanisms to support reporting of concerns.	PER	21.3.1 Procedures for Assessing Managing Ongoing Suitability	All entities
Develop clear processes for line managers to provide this information to security practitioners responsible for entity personnel security, and for the security practitioners to provide the information to the Authorised Vetting Agency.	PER	21.3.1.2. Performance Management	All entities
Provide line managers with guidance on identifying behaviours of concern and engaging in effective conversations about personnel security within the context of performance management. - Examples include confirming compliance with mandatory security awareness training, and ensuring understanding of reportable incidents and the contact reporting scheme.	PER	21.3.1.2. Performance Management	All entities
It is also important to identify gaps in knowledge about security, particularly where specialist knowledge or training is required to address entity-specific risks or in relation to compartmental briefings.	PER	21.3.1.2. Performance Management	All entities
The Sponsoring Entity should develop procedures and provide guidance for human resources areas to support information sharing arrangements and assist with identifying and communicating information.	PER	21.3.1.2. Performance Management	All entities
Entities should determine the frequency of periodic employment suitability checks based on the entity's risk profile as well as specific risks associated with the position, any associated enabling legislation and the entity's operating environment	PER	21.3.1.3. Periodic Employment Suitability Checks	All entities
Entities should explicitly agree on security clearance arrangements for personnel who are seconded, or are on temporary assignment, before the secondment or assignment commences.	PER	21.3.1.8. Clearance maintenance for personnel on secondment or temporary assignment	All entities
It may be appropriate to transfer sponsorship of the security clearance to the receiving entity for the period of the secondment or assignment (depending on the length of time and the level of access still required to the losing entity's resources).	PER	21.3.1.8. Clearance maintenance for personnel on secondment or temporary assignment	All entities
Authorised Vetting Agencies contact the Sponsoring Entity before commencing the revalidation of a security clearance to confirm the continuing security clearance requirements.	PER	21.5.1 Revalidation Timeframes	Authorised Vetting Agencies (AVA)
Entities identify and record positions that require a security clearance and the level of clearance required.	PER	21.5.1 Revalidation Timeframes	All entities
Entities ensure that each person working in an identified position have a valid security clearance issued by an Authorised Vetting Agency.	PER	21.5.1 Revalidation Timeframes	All entities
This responsibility extends to where a clearance holder's duties or role has changed. If a higher level clearance is required, a new clearance process will be necessary.	PER	21.5.1 Revalidation Timeframes	All entities
Consent should be obtained at key information collection points , such as pre-employment screening and application for a security clearance, and updated at reasonable intervals, such as when conducting periodic employment checks and revalidation of a security clearance.	PER	21.6.1.1. Consent	All entities
Negative Vetting 1 security clearance holders receive appropriate departmental travel briefings when undertaking international personal and work travel.	PER	21.7 International Travel	All entities
Procedures for managing personnel security during separation are established and tailored to the level of access to security classified information and resources, and the entity's assessment of the security risk.	PER	22 Separation	All entities
Risk assessment informs any security measures for personnel whose employment has been terminated, including security measures for high-risk personnel that may include immediate suspension of duties, immediate removal of all access to entity systems and facilities and escorting the person from the premises.	PER	22.1.1 Sharing Relevant Information	All entities
Entities provide personnel with an opportunity to confidentially express any security concerns relating to procedures or colleagues prior to separation.	PER	22.1.3 Security Concerns and Risks	All entities
Entities should consider the sequencing of withdrawal of access to resources.	PER	22.2 Withdrawal of Access	All entities
If the original National Police Check is not shared (as a result of Commonwealth spent convictions scheme requirements), the gaining Authorised Vetting Agency requests a new National Police Check on transfer of the personal security file.	PER	22.3.2 Personal Security File	All entities
Where there are concerns transferring personal security files, Authorised Vetting Agencies will advise the Sponsoring Entity. The Sponsoring Entity can then make a risk-based decision on providing or continuing access to Australian Government resources.	PER	22.3.2 Personal Security File	Authorised Vetting Agencies (AVA)
The gaining Authorised Vetting Agency should not request this information again, unless there are concerns about the authenticity of the documents originally supplied.	PER	22.3.2 Personal Security File	Authorised Vetting Agencies (AVA)
If electronic packs are used, information may be regathered electronically to populate the electronic record; this occurs at the next revalidation or review of the security clearance.	PER	22.3.2 Personal Security File	All entities

The losing Sponsoring Entity (the home entity), in consultation with the gaining Sponsoring Entity (the host entity) determine whether to treat a temporary transfer or secondment as a separation for the purpose of security clearance sponsorship. Relevant factors to consider include: - The duration of the transfer or secondment and the level of access personnel will require to the home entity and host entity resources during the transfer or secondment - Whether the host entity requires a security clearance for the position at the same, higher or lower level than the home entity - Whether both entities use the same Authorised Vetting Agency and if there is a need to transfer the clearance holder's personal security file.	PER	22.3.3 Temporary Transfer or Secondment	All entities
If the host entity requires a higher level of clearance or the clearance expires during the period of the temporary transfer, the host entity's Authorised Vetting Agency is responsible for the upgrade of the clearance.	PER	22.3.3 Temporary Transfer or Secondment	All entities
Entities take a risk-based approach to determine the length of leave that constitutes 'extended leave' by considering an entity's risk profile and any specific risks associated with the position. Generally, a period of three months or longer may be considered as extended leave.	PER	22.3.3.1. Extended leave	All entities
Entities advise the Authorised Vetting Agency to change clearances to inactive for personnel on extended absences based on their risk assessment. When clearance subjects return to work, the Authorised Vetting Agency can make the clearance active, if requested, after undertaking appropriate vetting updates.	PER	22.3.3.1. Extended leave	All entities
Entities include personnel security guidance on the following in their human resources or leave-related procedures: - notifying relevant security practitioners in advance of personnel commencing extended leave, as well as completing risk assessments if required - considering and managing security issues before extended leave is approved, particularly if it is assessed as likely that personnel may decide not to return (entities are encouraged to resolve any security issues before the leave commences) - reminding personnel on extended leave of their ongoing confidentiality obligations - briefing personnel travelling overseas of their responsibilities, including the requirement to report suspicious, unusual or persistent contacts, as well as contact with foreign nationals that becomes ongoing, and - advising the Authorised Vetting Agency when a security clearance holder is taking extended leave and requesting the clearance status be changed to inactive	PER	22.3.3.1. Extended leave	All entities
Ensuring recommencement procedures include changing the status of the security clearance and noting that the Authorised Vetting Agency may need to undertake vetting updates.	PER	22.3.3.1. Extended leave	All entities
The CSO and security practitioners should be involved in assessing the suitability of the physical security environment of a proposed site for entity facilities, and whether a facility can be constructed or modified to incorporate security measures that provide appropriate risk mitigation strategies.	PHYS	23.1.2 Facility Site Selection	All entities
Consider the location of vulnerable areas, such as mailroom and parcel delivery areas, that may be exposed to threats such as explosive devices, chemical, radiological and biological attacks, and apply appropriate physical mitigations (e.g. mail-screening devices, a stand-alone delivery area or using a commercial mail receiving area and sorting service).	PHYS	23.2 Design and Modify Entity Facilities	All entities
Store security classified information and resources security containers and cabinets separately from physical assets to lower the risk of compromise of information if valuable and attractive physical assets are stolen and assist investigators to determine the reason for the incidents involving unauthorised access.	PHYS	25.2 Security Containers, Cabinets and Rooms	All entities
Seek advice from qualified locksmiths or manufacturers when deciding the criteria to apply to select commercial safes and vaults.	PHYS	25.2.2 Commercial Safes and Vaults	All entities
Implement other physical controls that give the same level of intrusion resistance and delay where physical assets cannot be secured in commercial safes and vaults. These physical controls may include individual item alarms, alarm circuits or additional out-of-hours guarding.	PHYS	25.2.2 Commercial Safes and Vaults	All entities
Locate key cabinets within a facility's secure perimeter and, where possible, within the perimeter of the Security Zone where the locks are located.	PHYS	25.3.1 Restricted Keying Systems	All entities
Seek specialist advice in the design of closed circuit television management systems.	PHYS	25.5.1 Closed Circuit Television	All entities
Response time for off-site guards should be less than the delay given by the total of other controls.	PHYS	25.8.1 Out-of-Hours Security Guard Services	All entities
Guarding response time to alarms to should be within the delay period given by the physical security controls, although, the highest level of assurance is provided by on-site guards who can respond immediately, 24 hours, seven days a week.	PHYS	25.8.1 Out-of-Hours Security Guard Services	All entities
Determine the requirement for guards (their duties and the need for and frequency of patrols) on the level of threat and risk.	PHYS	25.8.1 Out-of-Hours Security Guard Services	All entities
Assess the security clearance requirement for guards based on the security zone requirements and frequency of access.	PHYS	25.8.1 Out-of-Hours Security Guard Services	All entities
Only employ, either through the entity or through a commercial guarding company, guards who are licensed in the jurisdiction where they are employed.	PHYS	25.8.1 Out-of-Hours Security Guard Services	All entities
Entities may, as a result of their risk assessment, consider that more frequent audits are appropriate for higher risk resources, for example valuable assets, attractive assets and assets of cultural significance.	PHYS	25.10.2 Asset Control for Physical Resources	All entities