Comparison of PSPF requirements

This document maps the 16 core requirements in the new Protective Security Policy Framework (PSPF) (which applies from 1 October 2018) to the 36 mandatory requirements found in the previous PSPF (prior to 30 September 2018).

Security Governance

PSPF mandatory requirement to 30 September 2018		PSPF core requirements from 1 October 2018
GOV-1	Agencies must provide all staff, including contractors, with sufficient information and security awareness training to ensure they are aware and meet the requirements of the Protective Security Policy Framework.	**Governance: Management structures and responsibilities**
GOV-2	To fulfil their security obligations, agencies must appoint: • a member of the Senior Executive Service as the security executive, responsible for the agency protective security policy and oversight of protective security practices • an agency security adviser (ASA) responsible for the day-to-day performance of protective security functions • an information technology security adviser (ITSA) to advise senior management on the security of the agency's Information Communications Technology (ICT) systems.	**Governance: Management Structures and responsibilities**
GOV-3	Agencies must ensure that the agency security adviser (ASA) and information technology security adviser (ITSA) have detailed knowledge of agency specific protective security policy, protocols and mandatory protective security requirements in order to fulfil their protective security responsibilities.	Nil
GOV-4	Agencies must prepare a security plan to manage their security risks. The security plan must be updated or revised every two years or sooner where changes in risks and the agency's operating environment dictate.	**Governance: Security planning and risk management**
GOV-5	Agencies must develop their own set of protective security policies and procedures to meet their specific business needs.	Nil
GOV-6	Agencies must adopt a risk management approach to cover all areas of protective security activity across their organisation, in accordance with the Australian Standards AS/NZS ISO 31000:2009 Risk management— Principles and guidelines and HB 167:2006 Security risk management.	Referred to in: • **Governance: Role of the accountable authority** • **Governance: Security planning and risk management**
GOV-7	For internal audit and reporting, agencies must: • undertake an annual security assessment against the mandatory requirements detailed within the Protective Security Policy Framework • report their compliance with the mandatory requirements to the relevant portfolio Minister The report must: • contain a declaration of compliance by the agency head • state any areas of non-compliance, including details on measures taken to lessen identified risks In addition to their portfolio Minister, agencies must send a copy of their annual report on compliance with the mandatory requirements to: • the Secretary, Attorney-General's Department • the Auditor General Agencies must also advise any non-compliance with mandatory requirements to: • the Director, Australian Signals Directorate for matters relating to the Australian Government Information Security Manual (ISM) • the Director-General, Australian Security Intelligence Organisation for matters relating to national security • the heads of any agencies whose people, information or assets may be affected by the non-compliance.	**Governance: Reporting on security**

PSPF mandatory requirement to 30 September 2018		PSPF core requirements from 1 October 2018
GOV-8	Agencies must ensure investigators are appropriately trained and have procedures in place for reporting and investigating security incidents and taking corrective action, in accordance with the provisions of the: • *Australian Government protective security governance guidelines— Reporting incidents and conducting security investigations*, or • *Australian Government Investigations Standards*.	Referred to in **Governance: Management structures and responsibilities**
GOV-9	Agencies must give all employees, including contractors, guidance on Sections 70 and 79 of the *Crimes Act 1914*, section 91.1 of the Criminal Code Act 1995, the *Freedom of Information Act 1982* and the Information Privacy Principles contained in the *Privacy Act 1988*, including how this legislation relates to their role.	Nil
GOV-10	Agencies must adhere to any provisions concerning the security of people, information and assets contained in multilateral or bilateral agreements and arrangements to which Australia is a party.	**Governance: Security governance for international sharing**
GOV-11	Agencies must establish a business continuity management (BCM) program to provide for the continued availability of critical services and assets, and other services and assets when warranted by a threat and risk assessment.	Nil
GOV-12	Agencies must ensure the contracted service provider complies with the requirements of this policy and any protective security protocols.	**Governance: Security Governance for contracted goods and service providers**
GOV-13	Agencies must comply with section 10 of the Public Governance, Performance and Accountability Rule 2014 and the Commonwealth Fraud Control Policy.	Nil

Information Security

PSPF mandatory requirement to 30 September 2018		PSPF core requirements from 1 October 2018
INFOSEC-1	Agency heads must provide clear direction on information security through the development and implementation of an agency information security policy, and address agency information security requirements as part of the agency security plan.	**Governance: Security planning and risk management**
INFOSEC-2	Each agency must establish a framework to provide direction and coordinated management of information security. Frameworks must be appropriate to the level of security risks to the agency's information environment.	Referred to in: • **Information security: Access to information** • **Governance: Security governance for contracted goods and service providers**
INFOSEC-3	Agencies must implement policies and procedures for the security classification and protective control of information assets (in electronic and paper-based formats), which match their value, importance and sensitivity.	**Information security: Sensitive and classified information**
INFOSEC-4	Agencies must document and implement operational procedures and measures to ensure information, ICT systems and network tasks are managed securely and consistently, in accordance with the level of required security. This includes implementing the mandatory *'Strategies to Mitigate Targeted Cyber Intrusions'* as detailed in the Australian Government Information Security Manual (ISM).	**Information security: Safeguarding information from cyber threats**
INFOSEC-5	Agencies must have in place control measures based on business owner requirements and assessed/accepted risks for controlling access to all information, ICT systems, networks (including remote access), infrastructures and applications. Agency access control rules must be consistent with agency business requirements and information classification as well as legal obligations.	**Information security: Access to information**
INFOSEC-6	Agencies must have in place security measures during all stages of ICT system development, as well as when new ICT systems are implemented into the operational environment. Such measures must match the assessed security risk of the information holdings contained within, or passing across, ICT networks, infrastructures and applications.	**Information security: Robust ICT systems**
INFOSEC-7	Agencies must ensure that agency information security measures for all information processes, ICT systems and infrastructure adhere to any legislative or regulatory obligations under which the agency operates.	Nil

Personnel Security

PSPF Mandatory requirement to 30 September 2018		PSPF Core requirements from 1 October 2018
PERSEC-1	Agencies must ensure that their personnel who access Australian Government resources (people, information and assets): • are eligible to have access • have had their identity established • are suitable to have access • agree to comply with the Government's policies, standards, protocols and guidelines that safeguard the agency's resources from harm.	**Personnel security: Eligibility and suitability of personnel**
PERSEC-2	Agencies must have policies and procedures to assess and manage the ongoing suitability for employment of their personnel.	**Personnel security: Ongoing assessment of personnel**
PERSEC-3	Agencies must identify, record and review positions that require a security clearance and the level of clearance required.	**Personnel security: Eligibility and suitability of personnel**
PERSEC-4	Agencies must ensure their personnel with ongoing access to Australian Government security classified resources hold a security clearance at the appropriate level, sponsored by an Australian Government agency.	**Information security: Sensitive and classified information**
PERSEC-5	Before issuing an eligibility waiver (citizenship or checkable background) and prior to requesting an Australian Government security clearance an agency must: • justify an exceptional business requirement • conduct and document a risk assessment • define the period covered by the waiver (which cannot be open- ended) • gain agreement from the clearance applicant to meet the conditions of the waiver • consult with the vetting agency.	**Personnel security: Eligibility and suitability of personnel**
PERSEC-6	Agencies, other than authorised vetting agencies, must use the Australian Government Security Vetting Agency (AGSVA) to conduct initial vetting and reviews.	**Personnel security: Eligibility and suitability of personnel**
PERSEC-7	Agencies must establish, implement and maintain security clearance policies and procedures for clearance maintenance in their agencies.	**Personnel security: Ongoing assessment of personnel**
PERSEC-8	Agencies and vetting agencies must share information that may impact on an individual's ongoing suitability to hold an Australian Government security clearance.	**Personnel security: Ongoing assessment of personnel**
PERSEC-9	Agencies must have separation policies and procedures for departing clearance holders, which includes a requirement to: • inform vetting agencies when a clearance holder leaves agency employment or contract engagement • advise vetting agencies of any security concerns.	**Personnel security: Separating personnel**

Physical Security

PSPF Mandatory requirement to 30 September 2018		PSPF Core requirements from 1 October 2018
PHYSEC-1	Agency heads must provide clear direction on physical security through the development and implementation of an agency physical security policy, and address agency physical security requirements as part of the agency security plan.	**Governance: Security planning and responsibilities**
PHYSEC-2	Agencies must have in place policies and procedures to: • identify, protect and support employees under threat of violence, based on a threat and risk assessment of specific situations. In certain cases, agencies may have to extend protection and support to family members and others • report incidents to management, human resources, security and law enforcement authorities, as appropriate • provide information, training and counselling to employees • maintain thorough records and statements on reported incidents.	Nil
PHYSEC-3	Agencies must ensure they fully integrate protective security early in the process of planning, selecting, designing and modifying their facilities.	**Physical security: Entity facilities**
PHYSEC-4	Agencies must ensure that any proposed physical security measure or activity does not breach relevant employer occupational health and safety obligations.	Nil

PSPF Mandatory requirement to 30 September 2018		PSPF Core requirements from 1 October 2018
PHYSEC-5	Agencies must show a duty of care for the physical safety of those members of the public interacting directly with the Australian Government. Where an agency's function involves providing services, the agency must ensure that clients can transact with the Australian Government with confidence about their physical wellbeing.	Nil
PHYSEC-6	Agencies must implement a level of physical security measures that minimises or removes the risk of information and ICT equipment being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.	**Physical security: Entity physical resources**
PHYSEC-7	Agencies must develop plans and procedures to move up to heightened security levels in case of emergency and increased threat. The Australian Government may direct its agencies to implement heightened security levels.	**Governance: Security planning and risk management**