Protective Security Policy Framework 2015-16 Compliance Report

Attorney-General's Department

Australian Attorney General's Department

Table of Contents

Protective Security Policy Framework 2015-16 Compliance Report

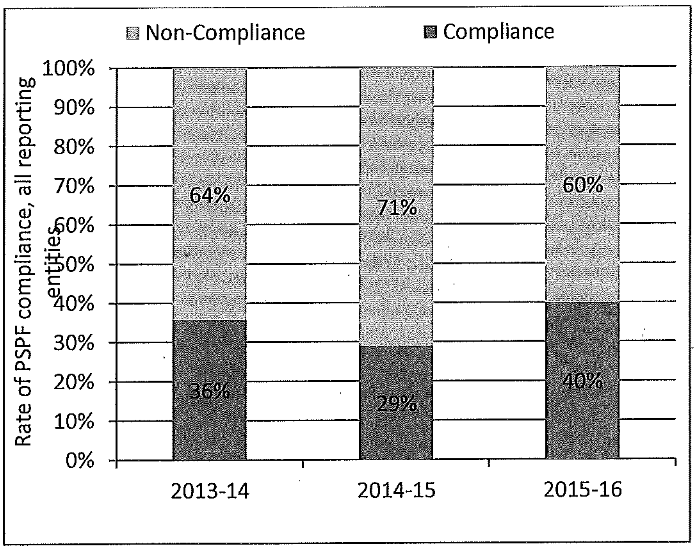
Key findings

The 2015-16 reporting period shows a marked increase in entity compliance compared to the 2014-15 reporting period. Overall levels of entity compliance have increased from 29 percent in 2014-15 to 40 percent in 2015-16 (see Figure 1).

Information security remains an ongoing challenge for the Australian Government (see Figure 2) with 35 percent of entities unable to fully implement the Australian Signals Directorate's (ASD) 'Top 4' strategies to mitigate targeted cyber intrusions, compared with 48 percent in 2014-15 (INFOSEC4, see Attachment A).

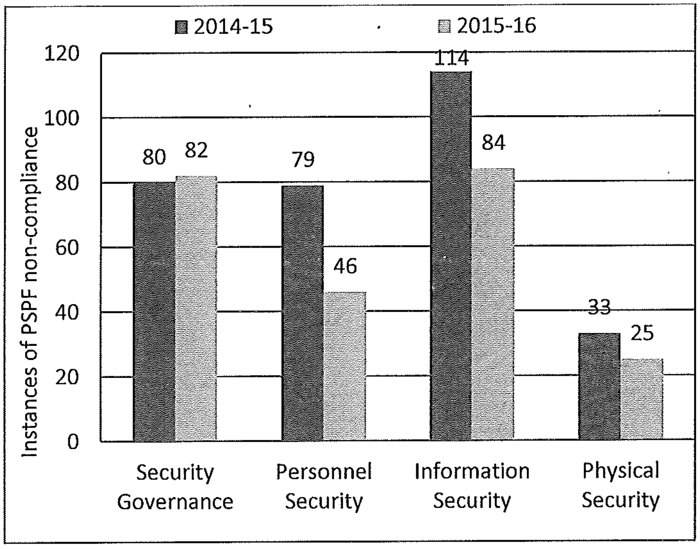
There have been notable improvements in personnel security compliance in 2015-16 compared to the 2014-15 reporting period. This is largely due to significant improvement in agency compliance with three additional personnel security requirements introduced in 2014, with only 17 agencies reporting non-compliance with one or more compared with 26 agencies in 2014-15 (see Figure 6).

Figure 1 Rate of entity compliance with the PSPF, 2013-14 to 2015-16



Compliance is measured by calculating the total number of reporting entities considered to be compliant with the PSPF.

Figure 2 Instances of non-compliance against PSPF components, 2014-15 and 2015-16



Instances of non-compliance include all non-compliance with a PSPF mandatory requirement reported by entities in this period.

Background

The Protective Security Policy Framework (PSPF) is administered by the Attorney-General's Department (AGD) and supports non-corporate Commonwealth entities to protect their people, information and assets, at home and overseas. It also provides assurance in information sharing, supports inter-entity business, helps meet international obligations, and more broadly enables the business of government. The PSPF mandates 36 overarching requirements to safeguard the Australian Government's personnel, information and assets. These requirements are described in full at Attachment A: PSPF Mandatory Requirements.

This report highlights significant trends identified by aggregate compliance data, including areas of non-compliance requiring additional government efforts to mitigate security risks. The report also details ongoing and agreed reforms to improve Australian Government protective security arrangements.

The PSPF applies to 94[1] non-corporate Commonwealth entities (NCCEs) subject to the ***Public Governance, Performance and Accountability Act 2013*** (PGPA Act), from national security entities, museums and media to health authorities. The PSPF represents better practice for corporate Commonwealth entities (CCEs) and wholly-owned Commonwealth companies under the PGPA Act.

The Attorney-General, as the responsible minister, has directed entity heads to implement effective protective security arrangements. Annual compliance reports assess:

- the effectiveness of the protective security policy as outlined in the PSPF's 36 mandatory requirements
- the extent to which entities have implemented the mandatory requirements and are compliant with Australian Government policy
- the adequacy of support and resources for entities' implementation of the policy, and
- where there is non-compliance, the barriers faced by the individual entity where applicable.

PSPF review

The 2015 APS-wide Independent Review of *Whole-of-Government Internal Regulation* (Belcher Review) examined the PSPF. The Belcher Review found that although the PSPF is underpinned by risk management principles there is confusion between mandatory and guidance elements, and policy prescription fostered a culture of 'tick-the-box' compliance, hampering effective engagement with risk.

In response to these findings, an AGD-convened review recommended simplifying the PSPF, removing duplication, increasing flexibility for entities to engage with risk, and incorporating new principles for decision-making, security outcomes and planning requirements. In May 2017 the Secretaries' Board considered the review outcomes and endorsed the direction of the proposed reforms. .

Entity reporting

Currently, annual PSPF compliance reporting relies on the accuracy of data provided to AGD by entities based on their assessment of compliance with the mandatory requirements. Australian National Audit Office (ANAO) reports have highlighted potential issues with the reliability of data gathered through self-assessed compliance reporting. To address this concern, entities are encouraged to have compliance reports audited, either independently or through internal audit functions.

NCCEs are required to report compliance with the PSPF to their Minister, the Secretary of AGD and ANAO on an annual basis. CCEs and Corporate companies are not required to implement or report against the PSPF, however a number have chosen to report on their compliance level against the PSPF as best practice.

A total of 105[2] NCCEs and CCEs reported their compliance against the PSPF in 2015-16 (see Table 1).

- Of the 94 NCCEs that reported in 2015-16, 36 self-assessed as fully compliant and 58 as non-compliant with at least one of the PSPF mandatory requirements.
- Of the 11 CCEs that reported, six self-assessed as compliant and five as non-compliant with the PSPF.
- One Corporate company reported against the draft Commonwealth Authorities and Companies (Application of Protective Security Policy Framework) General Policy Order 2013 (GPO), reporting adequate security controls in place and no material non-compliance with the GPO. This report has not been included in the aggregate compliance data.

[1] As at 1 July 2016 there were 94 non-corporate Commonwealth entities (NCCEs).

[2] Three entities failed to report on their compliance for the 2015-16 reporting period. Entities that failed to provide a compliance report are considered to be non-compliant with at least one requirement (GOV-7) of the PSPF and were reported as non-compliant with the PSPF.

Table 1 Number of PSPF report responses, 2013-14 to 2015-16

Entity type	2013-14	2014-15		2015-16	
	Reporting entities	Reporting entities	% entities fully compliant	Reporting entities	% entities fully compliant
Non-corporate Commonwealth entities (NCCE)*	104	95	29%	94	38%**
Corporate Commonwealth entities (CCE)*	8	9	33%	11	55%
Total reporting entities	**112**	**104**	29%	**105**	40%

* Variation in the number of entities reporting on their PSPF compliance between 2013-14 and 2015-2016 is due to machinery of government changes causing fluctuations in the number of NCCEs required to report against the PSPF and the number of CCEs that have self-nominated to report against the PSPF.

** Of the non-compliant entities, three entities were considered non-compliant due to failure to provide a report (PSPF mandatory requirement GOV-7).

2015-16 findings

There has been a significant increase in compliance levels across government, with the rate of non-compliance at the lowest level since the implementation of the PSPF in 2012-13. There was a drop in non-compliance from 71 percent in 2014-15 to 60 percent in 2015-16 as a proportion of all reporting entities (see Figure 1).

Information security continues to represent the highest level of overall non-compliance and remains an area of ongoing risk for the Australian Government (see Figure 2). Entities continue to find it challenging to implement ASD's 'Top 4' strategies to mitigate targeted cyber intrusions.

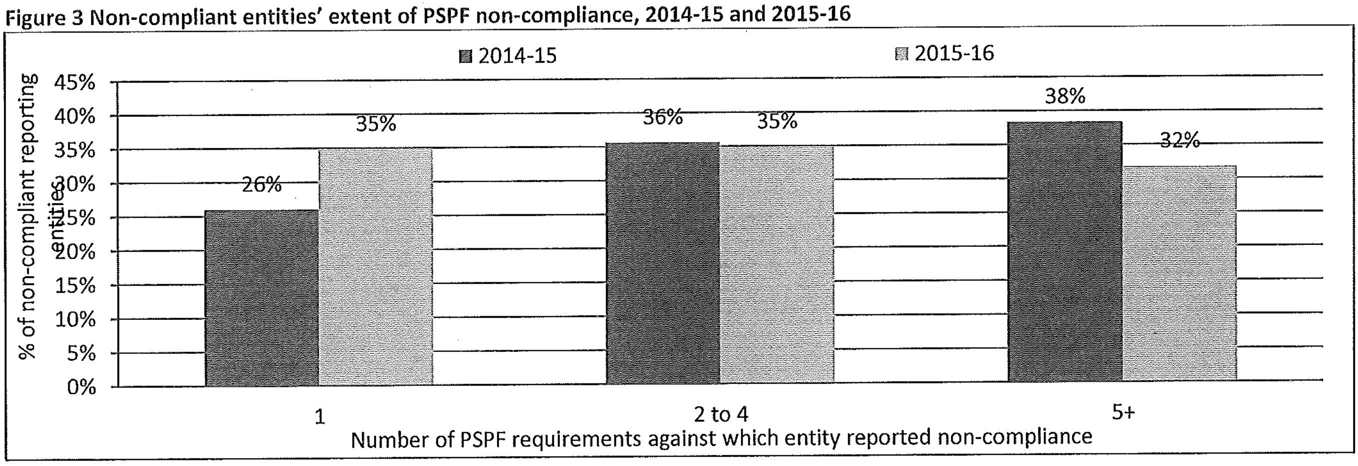
Changes in PSPF compliance

Table 2 Changes in PSPF compliance, 2014-15 to 2015-16

Change occurred	Number of entities
Non-compliant to compliant	**17**
Increasing compliance with requirements but remained non-compliant overall	**27**
Compliant to non-compliant	**5**
Non-compliance further deteriorated	**12**
No change	**40**
No compliance data is available for the remaining entities[3]	**4**

Overall, there was an improvement in entities' compliance with the PSPF in comparison with the 2014-15 period. One entity reported non-compliance with 17 mandatory requirements in 2015-16, being the most significant report of non-compliance in any period to date. This entity is undertaking a comprehensive review of its security procedures and operations aiming to significantly improve compliance across the mandatory requirements by 30 June 2017. AGD has offered the entity assistance to achieve an increase in compliance.

Figure 3 Non-compliant entities' extent of PSPF non-compliance, 2014-15 and 2015-16



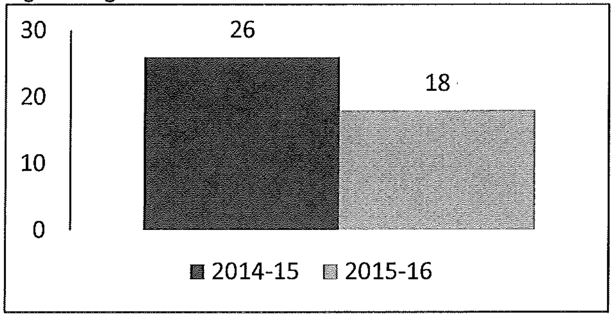
[3] Due to classified compliance reporting in 2015-16 or no response from some NCCEs or CCEs in 2015-16.

'At risk' entities

AGD uses compliance reporting to identify entities that are most significantly 'at risk' based on three criteria:

- non-compliance with 10 or more mandatory requirements
- non-compliance with the requirement to adopt a risk management approach (GOV-6), and
- a decline in entity compliance by three or more mandatory requirements over the previous year.

Figure 4 Agencies assessed as 'At Risk' in 2014-15 and 2015-16

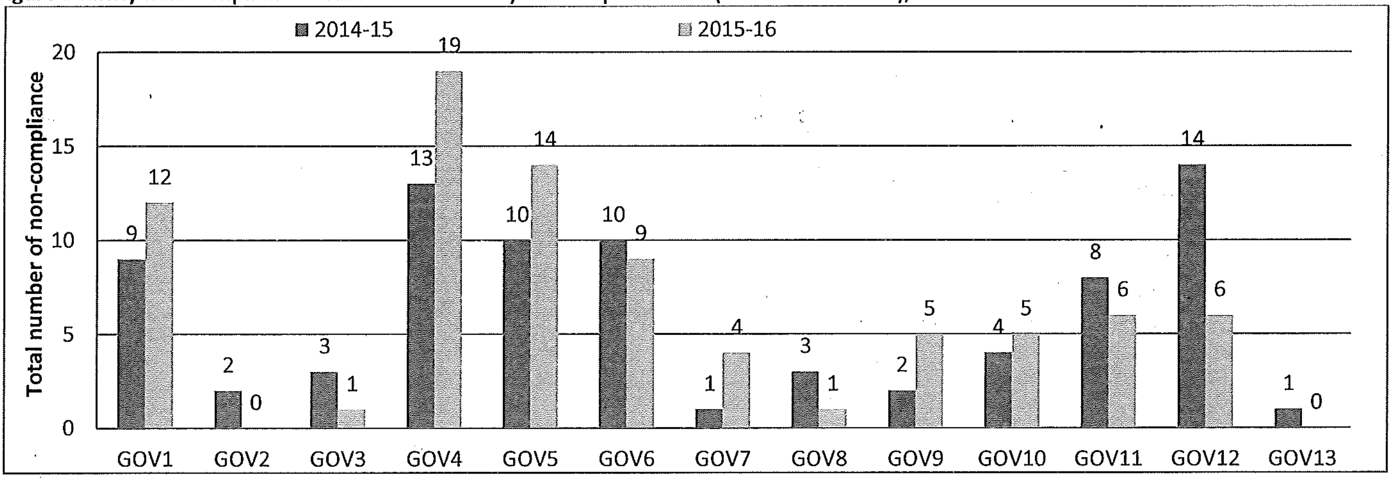


Compliance against PSPF components and mandatory requirements

Governance (GOV)

Compliance levels with governance requirements fluctuated during the 2015-16 period with significant improvements with entities ensuring contracted service providers complied with the PSPF (GOV-12) and entities complying with the Commonwealth Fraud Control Framework (GOV-13). Compliance levels in security awareness training (GOV-1), planning (GOV- 4) and developing agency specific procedures (GOV- 5) declined (see Figure 5). Overall, governance requirements represent the second highest level of non-compliance. Further work on outreach strategies aimed to improve security culture across government was agreed as part of the Personnel Security Reforms endorsed by Government in 2016. These strategies are currently being implemented.

Figure 5 Entity non-compliance with PSPF mandatory GOV requirements (see Attachment A), 2014-15 and 2015-16

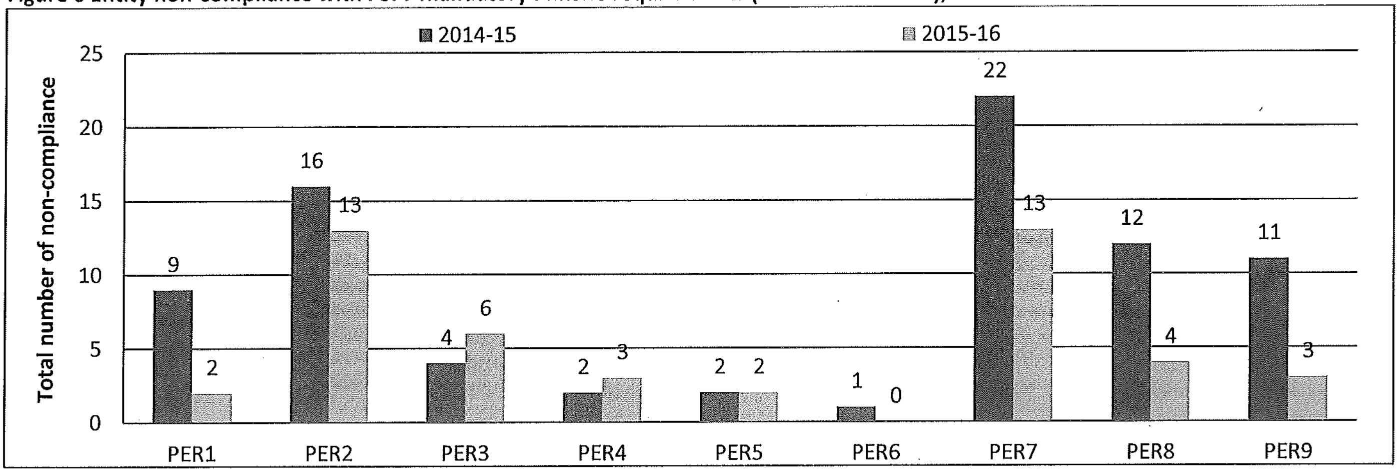


* refer to Attachment A for descriptions for each mandatory requirement.

Personnel security (PERSEC)

Personnel security arrangements provide entities with a level of assurance as to the eligibility, suitability and assessment expectations of a person accessing Australian Government resources. This is the second reporting period entities have been required to assess compliance against three additional personnel security requirements (PERSEC-7-9) introduced in 2014. These requirements include having effective security clearance policies, sharing information between agencies and vetting agencies and establishing separation policies and procedures. A significant improvement in entity compliance with these three PERSEC requirements has been recorded in 2015-16 (see Figure 6). Overall, personnel security has the second highest level of compliance in this reporting period.

Figure 6 Entity non-compliance with PSPF mandatory PERSEC requirements (see Attachment A), 2014-15 and 2015-16



* refer to Attachment A for descriptions for each mandatory requirement.

Eligibility waivers of PERSEC vetting requirements

Australian Government security clearances subject to eligibility waivers represent a vulnerability to exploitation from organised crime and foreign governments. Entities reported a 41 percent decline in waivers held between 2014-15 and 2015-16 (see Table 3).

Table 3 Waivers of vetting requirements, 2014-15 to 2015-16

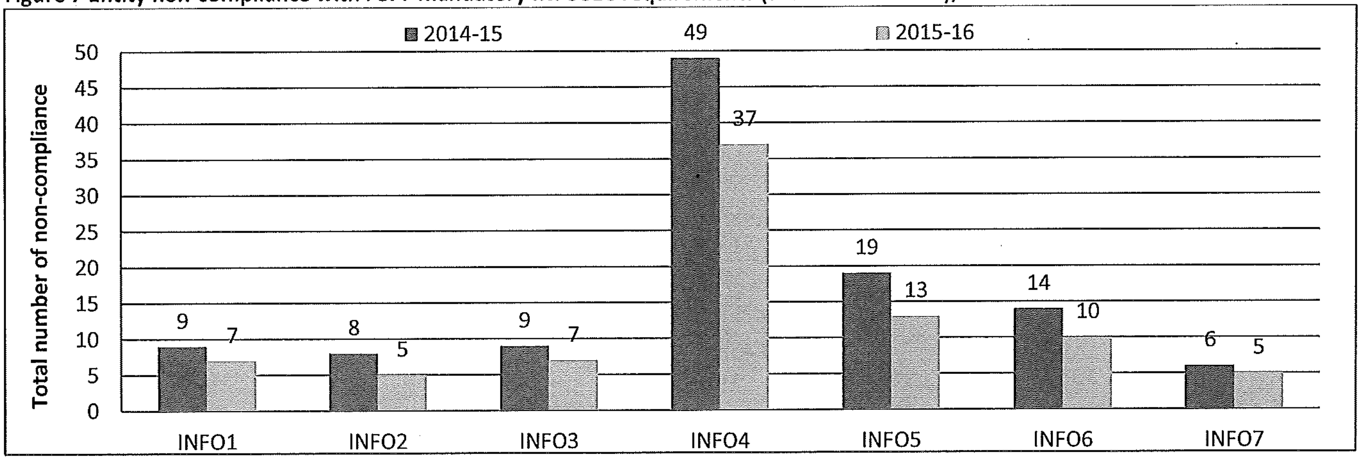
Year	Number of waivers reported
2014-15	177
2015-16	105

Information security (INFOSEC)

Information security is a dynamic policy area which requires agility and flexibility to meet challenges posed by continuous technological advancement. In 2015-16, improvements have been recorded in compliance across information security, although it remains the PSPF component with the lowest level of compliance.

Implementation of the 'Top 4' strategies mitigate 85 percent of risks posed by targeted cyber intrusions and achieving and maintaining high levels of compliance against this requirement should remain a priority for entities. The 2015-16 data indicates that information security is an ongoing risk for the Australian Government with 35 percent of entities reporting non-compliance with INFOSEC-4 (see Attachment A). However, this has been an improvement from 2014-15 with only 53 percent of entities compliant with this requirement in this period. Twenty percent of those reporting non-compliance reported INFOSEC-4 as their only area of non-compliance against the PSPF.

Figure 7 Entity non-compliance with PSPF mandatory INFOSEC requirements (see Attachment A), 2014-15 and 2015-16



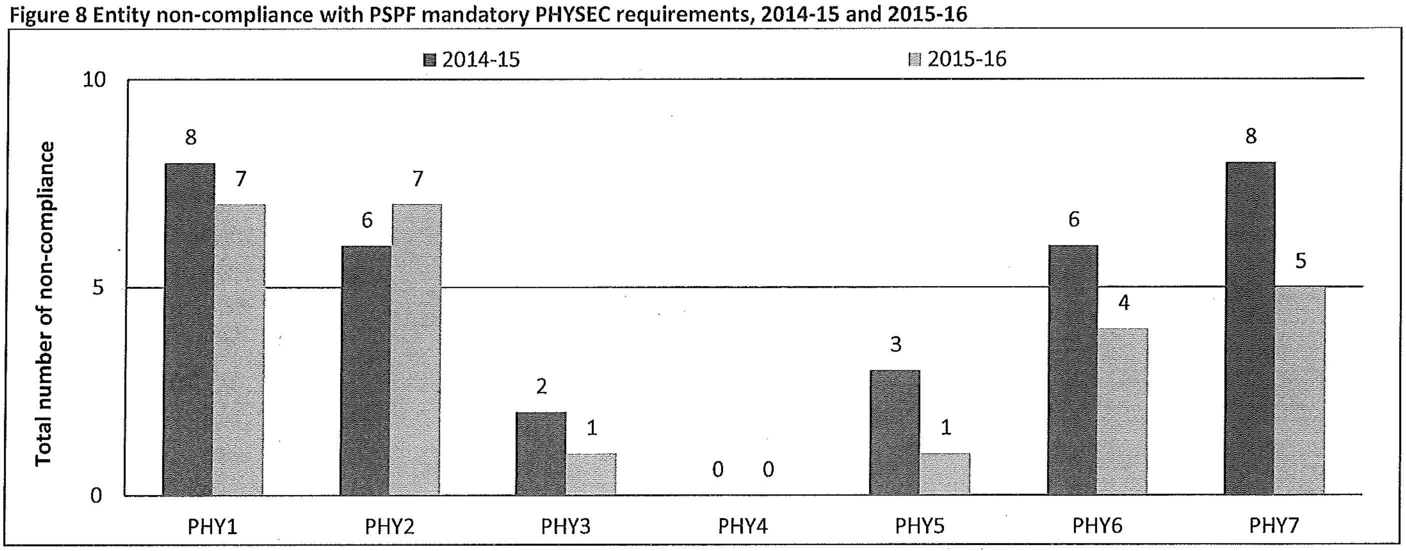
* refer to Attachment A for descriptions for each mandatory requirement.

ASD's recently introduced 'Essential Eight' incorporated but do not replace the 'Top 4', however, entities identifying significant information security threats may wish to consider implementing the 'Essential Eight' as part of a their risk based approach to security management.

Physical security (PHYSEC)

Physical security elements of the PSPF are a combination of physical and procedural measures that entities adopt to mitigate the risk of compromise by physical means of its people, information and assets. In 2015-16, physical security again has the highest level of compliance of any PSPF component.

Figure 8 Entity non-compliance with PSPF mandatory PHYSEC requirements, 2014-15 and 2015-16



* refer to Attachment A for descriptions for each mandatory requirement.

Compliance by function

In 2015-16, approximately half of all regulatory and specialist entities reported compliance with the PSPF in comparison with 31 percent of policy entities and only 15 percent of operational entities. Data indicates that operational entities find it significantly more difficult to implement the 'Top 4' mandated by INFOSEC-4, with 68 percent of operational entities recording non-compliance with INFOSEC-4 compared with only 28 percent of all other entities.

Next Steps

As part of the proposed PSPF reforms developed in response to the Belcher review recommendations, AGD is working with stakeholders to develop a maturity model for annual PSPF reporting during 2017-18 for implementation in the 2018-19 period. By reducing the focus on compliance based reporting, AGD aims to provide more useful reporting on the way entities implement the policy and engage with risk, while providing assurance to government that appropriately robust security arrangements are in place. This will be achieved by:

- enabling entities to report on outcomes relevant to risks, rather than relying on compliance for assurance
- enabling AGD to collect a more nuanced data set to target support to entities and allow benchmarking
- providing more relevant feedback to entities and enabling benchmarking, and
- informing policy review if entities continue to fail to improve their level of maturity.

Attachment A: PSPF Mandatory Requirements

Governance	
GOV-1	Entities must provide all staff, including contractors, with sufficient information and security awareness training to ensure they are aware of, and meet the requirements of the Protective Security Policy Framework.
GOV-2	To fulfil their security obligations, entities must appoint: • A member of the Senior Executive Service as the security executive, responsible for the entity protective security policy and oversight of protective security practices. • An entity 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 entity's Information Communications Technology (ICT) systems.
GOV-3	Entities must ensure that the entity security adviser (ASA) and information technology security adviser (ITSA) have detailed knowledge of entity specific protective security policy, protocols and mandatory protective security requirements in order to fulfil their protective security responsibilities.
GOV-4	Entities 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 entity's operating environment dictate.
GOV-5	Entities must develop their own set of protective security policies and procedures to meet their specific business needs.
GOV-6	Entities 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.*
GOV-7	For internal audit and reporting, entities 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 entity head • state any areas of non-compliance, including details on measures taken to lessen identified risks. In addition to their portfolio Minister, entities must send a copy of their annual report on compliance with the mandatory requirements to: • the Secretary, Attorney-General's Department, and • the Auditor General. Entities 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, and • the heads of any entities whose people, information or assets may be affected by the non-compliance.
GOV-8	Entities 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,* and/or • *Australian Government Investigations Standards.*
GOV- 9	Entities must give all employees, including contractors, guidance on Sections 70 and 79 of the *Crimes Act 1914*, section 91 of the *Criminal Code Act 1995*, the *Freedom of Information Act 1982* and the Australian Privacy Principles contained in the *Privacy Act 1988,* including how this legislation relates to their role.
GOV-10	Entities 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.

GOV-11	Entities 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.
GOV-12	Entities must ensure the contracted service provider complies with the requirements of this policy and any protective security protocols.
GOV-13	Entities must comply with section 10 of the *Public Governance, Performance and Accountability Rule 2014* and the *Commonwealth Fraud Control Policy.*
Personnel Security	
PERSEC-1	Entities 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, and • agree to comply with the Government's policies, standards, protocols and guidelines that safeguard that entity's resources from harm.
PERSEC-2	Entities must have policies and procedures to assess and manage the ongoing suitability for employment of their personnel.
PERSEC-3	Entities must identify, record and review positions that require a security clearance and the level of clearance required.
PERSEC-4	Entities 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 entity.
PERSEC-5	Before issuing an eligibility waiver (citizenship or checkable background) and prior to requesting an Australian Government security clearance an entity 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 entity
PERSEC-6	Entities, other than authorised vetting entities, must use the Australian Government Security Vetting Entity (AGSVA) to conduct initial vetting and reviews.
PERSEC-7	Entities must establish, implement and maintain security clearance policies and procedures for clearance maintenance in their entities.
PERSEC-8	Entities and vetting entities must share information that may impact on an individual's ongoing suitability to hold an Australian Government security clearance.
PERSEC-9	Entities must have separation policies and procedures for departing clearance holders, which includes a requirement to: • inform vetting entities when a clearance holder leaves entity employment or contract engagement • advise vetting entities of any security concerns
Information Security	
INFOSEC-1	Entity heads must provide clear direction on information security through the development and implementation of an entity information security policy, and address entity information security requirements as part of the entity security plan.
INFOSEC-2	Each entity 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 entity's information environment.
INFOSEC-3	Entities 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.
INFOSEC-4	Entities 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.
INFOSEC-5	Entities 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. Entity access control rules must be consistent with entity business requirements and information classification as well as legal obligations.
INFOSEC-6	Entities 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.
INFOSEC-7	Entities must ensure that entity information security measures for all information processes, ICT systems and infrastructure adhere to any legislative or regulatory obligations under which the entity operates.
Physical Security	
PHYSEC-1	Entity heads must provide clear direction on physical security through the development and implementation of an entity physical security policy, and address entity physical security requirements as part of the entity security plan.
PHYSEC-2	Entities 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, entities 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, and • maintain thorough records and statements on reported incidents.
PHYSEC-3	Entities must ensure they fully integrate protective security early in the process of planning, selecting, designing and modifying their facilities.
PHYSEC-4	Entities must ensure that any proposed physical security measure or activity does not breach relevant employer occupational health and safety obligations.
PHYSEC-5	Entities must show a duty of care for the physical safety of those members of the public interacting directly with the Australian Government. Where an entity's function involves providing services, the entity must ensure that clients can transact with the Australian Government with confidence about their physical wellbeing.
PHYSEC-6	Entities 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.
PHYSEC-7	Entities 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 entities to implement heightened security levels.