Australian Government
Attorney-General's Department

Protective Security Policy Framework:
2017–18 Compliance Report

Attorney-General's Department

Protective Security Policy Framework

2017–18 Compliance Report

Introduction

Protecting the security of the Commonwealth's people, information and assets is fundamental to the secure and efficient delivery of government business. It is essential to building and maintaining trust and confidence between different levels of government, the Australian people and our international partners.

The Protective Security Policy Framework (PSPF) is administered by the Attorney-General's Department (AGD) and applies to non-corporate Commonwealth entities (NCCEs) that are subject to the *Public Governance, Performance and Accountability Act 2013* (PGPA Act).[1] The PSPF also represents better practice for corporate Commonwealth entities (CCEs) and wholly-owned Commonwealth companies under the PGPA Act.

For the 2017–18 reporting period, the PSPF mandated 36 security requirements to support government entities identifying threats and managing risks that have the potential to:

- harm staff or the public
- compromise official information or assets, or
- interrupt progress towards meeting government policy objectives.

Entities are required to undertake an annual self-assessment of their PSPF compliance and report on their security posture, providing details of measures taken to address identified key risks. The 36 requirements, and compliance with these requirements, is set out at **Attachment A**.

Implementing a new framework

The 2017–18 compliance report will be the final reporting period using the old framework. On 1 October 2018, a new PSPF commenced which takes into account recommendations contained in the *Independent Review of Whole-of-Government Internal Regulation* (Belcher Review). The reforms to the PSPF improve clarity, reduce unnecessary 'red tape' and foster a strengthened security culture across government. Entities will assess their security performance against 16 core requirements. The reforms to the PSPF do not fundamentally change entities' responsibilities to protect their people, information and assets.

From 2018–19, entities will report on their PSPF implementation using a security maturity model to assess the maturity of their protective security practices instead of a compliance model. A security maturity model aims to embed a stronger security culture by encouraging entities to continuously engage in identifying and assessing the risks present in their security environment. It also provides entities with the tools to assess their security performance in a more graded and relevant way, including how effectively they manage key risks and vulnerabilities.

Alongside the new maturity model, other recent developments to strengthen our security culture have been the establishment of the Chief Security Officer forums (SES level forums held twice a year) and reinvigorated communities of practice on security culture, vetting and personnel to provide a dedicated forum for security practitioners to exchange ideas and lessons.

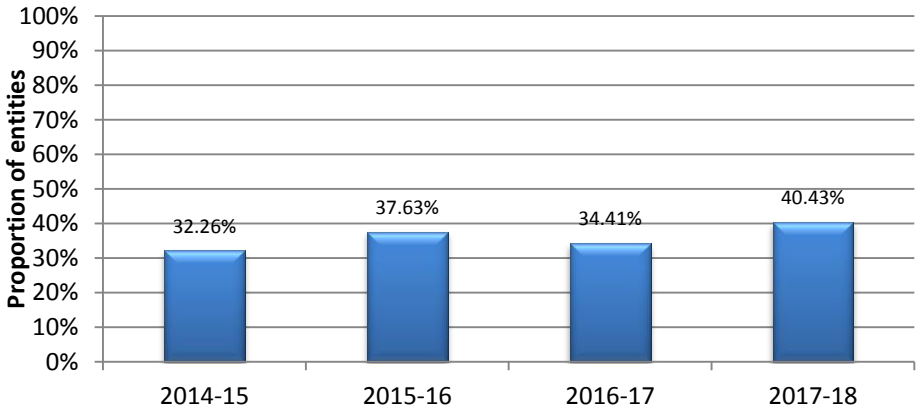
[1] There were 94 NCCEs as at 1 July 2018.

Key Findings: 2017–18

PSPF compliance

As in 2016–17, all NCCEs submitted a PSPF compliance report for the 2017–18 reporting period. In addition to this, eight CCEs voluntarily submitted compliance reports (up from six CCEs in 2016–17).

Figure 1: Proportion of NCCEs fully compliant with all PSPF requirements

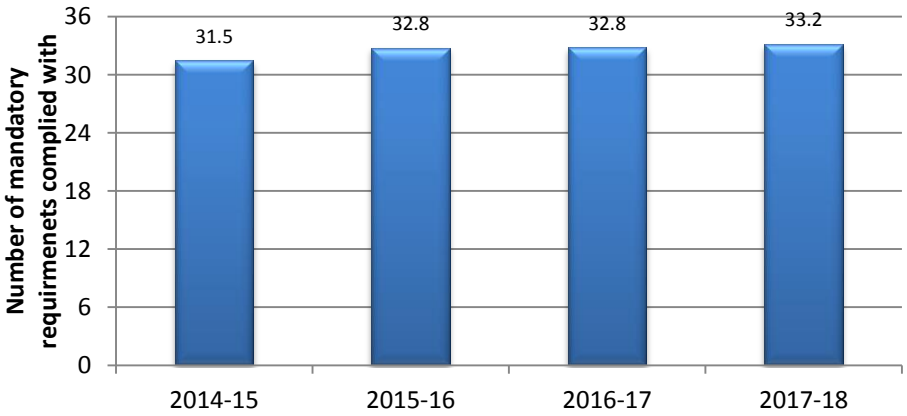


In 2017–18 the proportion of NCCE reports indicating full compliance with all PSPF requirements was 40.43%, up from 34.41% in 2016–17.

The 2017–18 reporting period shows an increase in the number of NCCEs reporting full compliance with all mandatory PSPF requirements from 34.41% fully compliant NCCEs in 2016–17 (n=93) to 40.43% fully compliant NCCEs in 2017–18 (n=94).

While full PSPF compliance was only reported by 40.43% of NCCEs, the Government's security posture is still broadly sound across the areas of security governance, personnel security, information security and physical security. On average in 2017–18, NCCEs reported compliance with 92.17% of the PSPF's requirements, equivalent to 33.2 of the 36 PSPF requirements (shown as '2017–18 compliance average' in Figures 3, 4, 5, 6 and 7). This builds on the 2016–17 average compliance of 91.22% by all NCCEs, equivalent to 32.8 of the 36 PSPF requirements.

Figure 2: Average number of PSPF requirements complied with by NCCEs



On average NCCE reports indicated compliance with 33.2 of the 36 PSPF requirements, above 2016-17 compliance of 32.8 of the 36 requirements. This represents an average of 92.17% compliance with the PSPF requirements.

Key risk areas

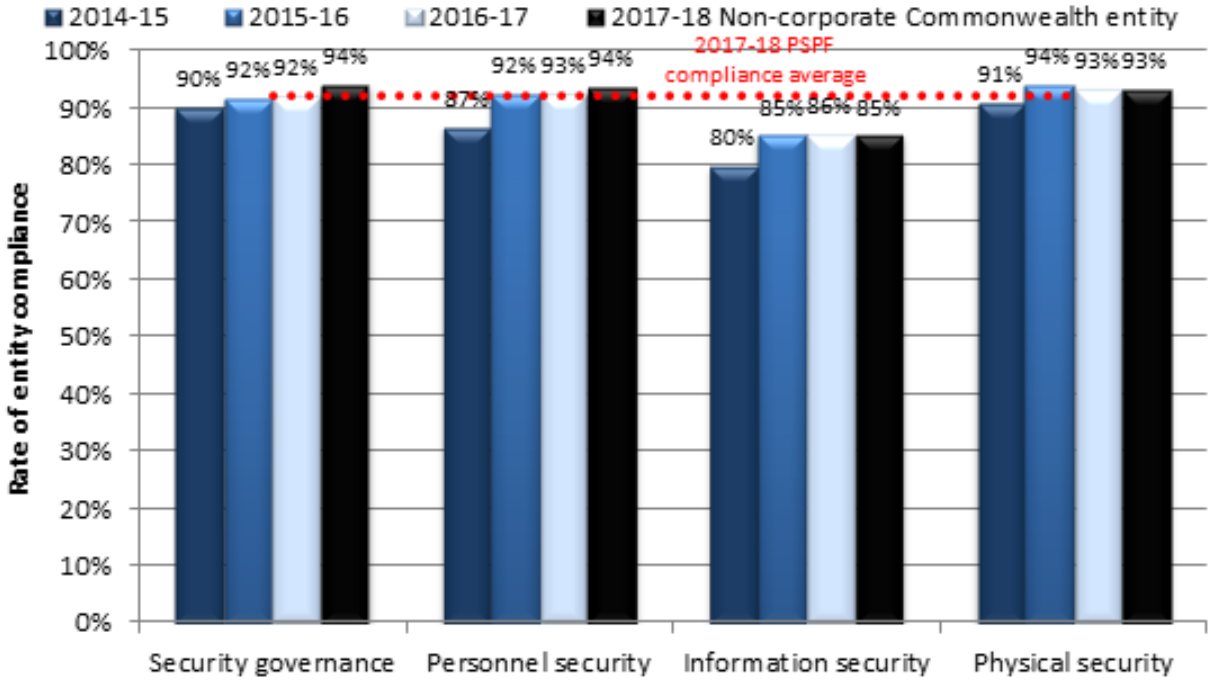
Of the four focus areas for protective security, information security remains an ongoing challenge for the Australian Government, with NCCEs reporting an average compliance of 85.26% for the PSPF information requirements. Of note, in 2017–18, there was a 5.19% reduction in average compliance levels with INFOSEC3. INFOSEC-3 contains policies and procedures for the security classification and protective control of information assets. Issues identified by NCCEs included gaps in their approaches to ensuring appropriate levels of protection are in place for information assets, and the introduction of new information assets (for example, introduction of tablets with voice and video conferencing capabilities) requiring entities to review their policies and procedures to ensure they have appropriate security classification and protective control of these information assets. The affected entities reported that they have measures in place to mitigate the associated risks from the identified non-compliance.

Levels of compliance with INFOSEC-4, relating to cyber and ICT system security, including the Australian Signals Directorate's *Strategies to Mitigate Targeted Cyber Incidents*, remain relatively steady, but continue to present an area of risk for the Australian Government with a level of compliance at 61.70%.

Compliance by PSPF requirement

The PSPF's 36 mandatory requirements cover four key areas: security governance, information security, personnel security, and physical security. This report provides an update on average compliance rates for all NCCEs across each of the four key areas and then further detail on compliance against each of the 36 individual requirements (which is primarily set out in the annexure). The level of NCCE compliance across all four key areas is generally high. Compliance with information security policy has the lowest level of compliance at 85.26% of the total 7 information security requirements. This equates to an average entity compliance with 6 of the total 7 information security requirements.

Figure 3: Proportion of PSPF requirements that NCCEs complied with by requirement areas



Compliance with information security requirements remains the lowest across all four PSPF requirement areas, at 85.26%.

NB: percentages in Figure 3 have been rounded to the nearest whole percentage.

Security governance

Compliance with PSPF security governance requirements remained high, a trend consistent with past reporting periods. The average level of compliance across all 13 security governance requirements was higher than any other area in the 2017–18 reporting period. The average level of compliance increased from 92.14% in 2016–17, equating to an average compliance with 12 of the 13 security governance requirements to 94.11% in 2017–18, equating to an average compliance with 12.2 of the 13 security governance requirements.

Of note, all NCCEs reported 100% compliance with three PSPF requirements, all of which were security governance requirements. These requirements were:

- GOV-2 relating to the requirement to appoint an entity security executive and supporting advisers
- GOV-7 relating to the obligation to undertake annual PSPF compliance reporting, and
- GOV-13 relating to implementing appropriate fraud controls.

Overall, the level of compliance remained stable or improved across all 13 security governance requirements, including a 5.42% increase in the level of compliance with GOV-11, the policy on establishing and maintaining an appropriate business continuity plan. This increase in GOV-11 compliance in the 2017–18 period can be attributed to seven of the nine entities reporting non-compliance with GOV-11 in 2016–17 implementing Business Continuity Management programs during 2017–18.

Personnel security

There was a marginal increase in the overall level of compliance with personnel security requirements, improving from 92.59% compliance, equating to an average of 8.3 of the 9 personnel security requirements in 2016–17 to 93.97% compliance, equating to an average of 8.5 of the 9 personnel security requirements for the 2017–18 reporting period. Compliance levels for PERSEC-7, outlining the policy on security clearances and procedures, remained the lowest across all nine personnel security requirements at 89.36%, which is consistent with trends across the compliance levels with PERSEC policies over the last four reporting periods.

Personnel security waivers

Access to classified resources is subject to personnel successfully undergoing a vetting process and holding a valid security clearance. Where security clearance eligibility requirements are waived, government may face increased malicious insider risks. There are two types of waiver:

- waiver of the **Australian citizenship requirement**, and
- waiver of the **checkable background requirement**.

A waiver can only be issued if there is an exceptional business requirement and the entity has conducted a risk assessment. An eligibility waiver is role-specific, non-transferable, finite and subject to the annual review. Security clearances granted on the basis of a citizenship or checkable background waiver cannot be transferred to a new position or entity unless the exceptional business requirement and risk assessment provisions are undertaken and accepted for the new position or entity.

The number of citizenship and checkable background waivers decreased substantially from the previous reporting period. Clearance holders with a waiver make up less than 0.1% of the approximately 400,000 active clearances across entities.[2]

Waivers of the Australian citizenship requirement

In 2017–18, there were 282 waivers of the Australian citizenship requirement for staff of NCCEs. This was a decrease of 35 waivers (11.04%) from the 2016–17 reporting period's total of 317 waivers.

A security risk may exist when a clearance subject is not an Australian citizen. A clearance subject who indicates a preference for a foreign country over Australia may be prone to act in ways that are harmful to the national interest of Australia. This situation could potentially introduce foreign influence that could result in the compromise of security classified information.

Table 1: Clearances with a citizenship waiver

Citizenship waivers	2016–17	2017–18
Baseline	124	181
NV1	175	68
NV2	14	19
PV	4	14
Total	**317**	**282**

There was a reduction in the number of security clearances with a citizenship waiver from the previous year (282 in 2017-18, down from 317 in 2016-17). A significant portion of this reduction can be attributed to a single entity resolving security clearance processes from the 2016-17 reporting period.

[2] This figure is approximate and was current as at April 2019.

Waivers of the checkable background requirement

Assurance about a person's background gives confidence that they can be trusted to protect government resources (people, information and assets). A person is considered to have an uncheckable background where more than 12 months (cumulative) of the security clearance background checking period cannot be verified.

In 2017–18, there were 117 security clearance holders with an uncheckable background. This is a 45.83% decrease in checkable background waivers from the 2016–17 figures of 216.

Table 2: Clearances with a checkable background waiver

Checkable Background waiver	2016–17	2017–18
Baseline	8	3
NV1	137	42
NV2	8	3
PV	63	69
Background Total	216	117

There was a 45.83% reduction in the number of checkable background waivers from 216 in 2016–17 to 117 in 2017–18. The majority of this reduction was at the NV1 security clearance level and can be attributed to a single entity.

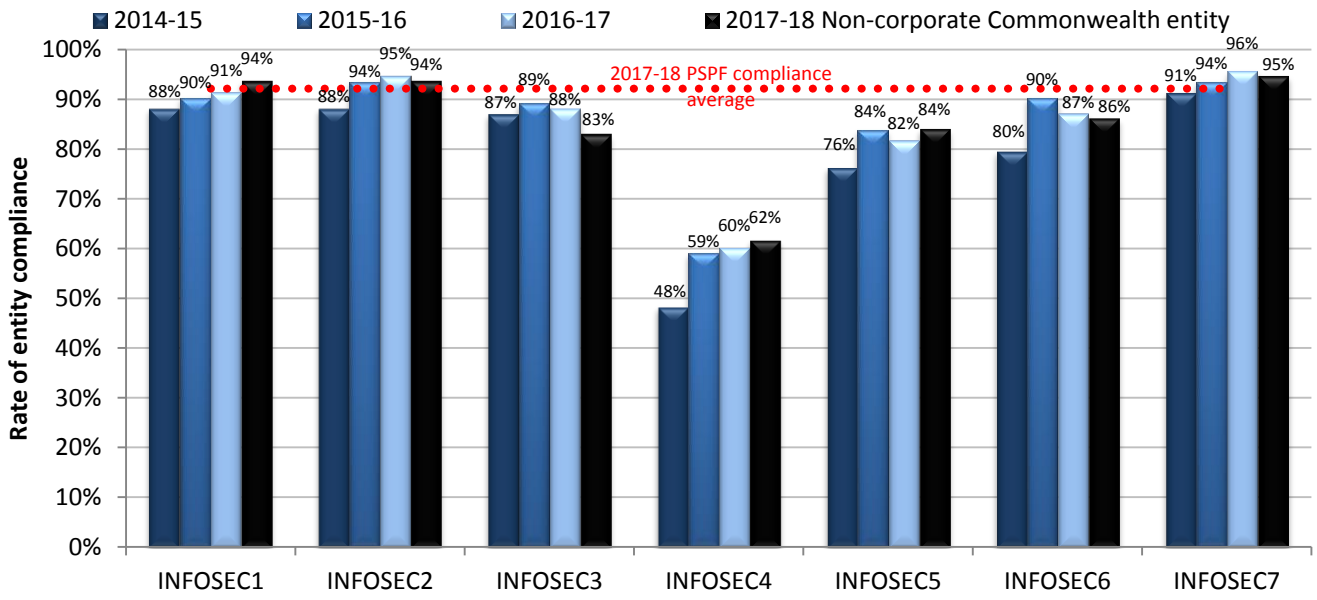
Checkable background waivers are most commonly granted for Positive Vetting (PV) level clearances. This reflects the more onerous background checking requirements accompanying a PV level clearance.[3]

Information security

Continuing advances in technology contribute to the dynamic environment of information security and the diverse threats encountered by the Australian Government in securing its information. As such, information security arrangements are an important element in an entity's effective protective security regime but a particularly challenging one.

Compliance with information security requirements remains an area of focus for all NCCEs.

Figure 4: Proportion of NCCEs compliant with PSPF INFOSEC requirements



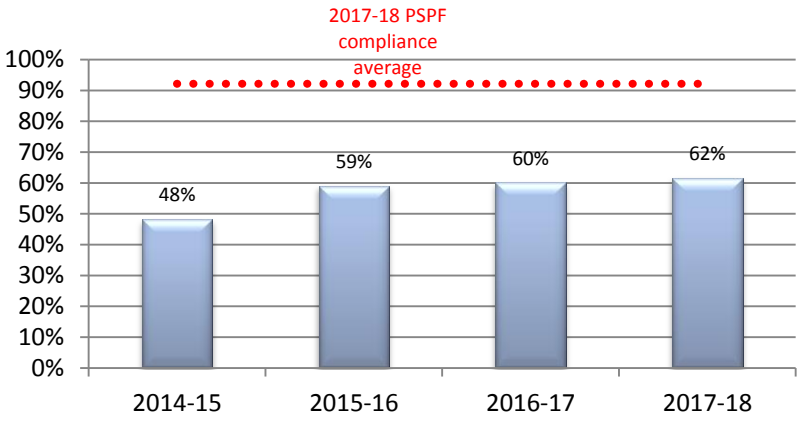
With increased awareness of cyber security risks and efforts highlighting appropriate risk mitigation strategies in 2016–17, entities were more considered in their assessment against the information security requirements recording no significant improvement in NCCE compliance with information security requirements in 2017–18.

[3] The 12 month cumulative threshold for the checkable background requirement means no more than 10% of a person's background can be uncheckable at the NV2 level without a waiver compared with 20% or a person's background at the Baseline level. For background checking requirements at the PV level, the 12 month cumulative threshold may represent a much smaller percentage of the person's background.

While there was a marginal increase in compliance with INFOSEC-4 from the 2016–17 reporting period (an improvement of 1.49%), at 61.70%, the level of INFOSEC-4 compliance remains the lowest of all 36 mandatory requirements. INFOSEC-4 sets out the requirements for implementing cyber and ICT system security, including the Australian Signal Directorate's *Strategies to Mitigate Cyber Security Incidents*.

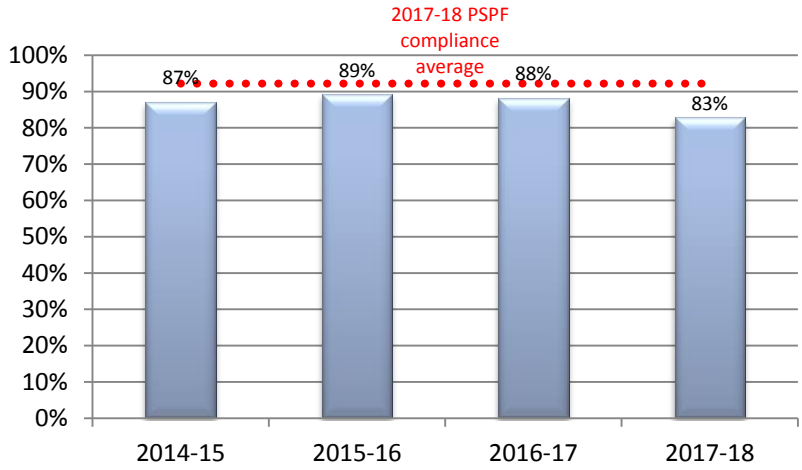
Compliance with INFOSEC-3, the policy concerning entities' security classification and the protective control of information assets, decreased by 5.19%. This is the only requirement in 2017–18 to record a decrease in the level of compliance of more than five percent. This change is attributed to some entities identifying gaps in their approaches following review of their policies and security measures regarding appropriate levels of protection for information assets. Also, with the introduction of new information assets, such as information platforms (windows tablets with voice and video conferencing capabilities), these affected entities are reviewing their policies and procedures with respect to security classification and protective control of these new information assets. The relevant entities reported that they have measures in place to mitigate the associated risks from their non-compliance.

Figure 5: Proportion of NCCEs compliant with PSPF INFOSEC-4



Implementation of the INFOSEC-4 requirement remains a key challenge across the NCCEs.

Figure 6: Proportion of NCCEs compliant with PSPF INFOSEC-3



INFOSEC-3 was the only PSPF mandatory requirement that saw a decrease in compliance of more than 5% from the 2016–17 reporting period.

Physical security

NCCEs continued to report high levels of compliance against the PSPF's physical security requirements. In 2017–18 NCCEs complied with 93.16% of the physical security requirements equating to compliance with 6.5 of the 7 physical security requirements. Although on average this is the same level of compliance with the physical security requirements as the 2016–17 compliance levels, there was a small decline of 0.23% in compliance levels from 2016-17 to 2017-18 due to the total number of NCCEs increasing from 93 to 94.

Of particular note, over 98.94% of NCCEs reported full compliance with PHYSEC-4, ensuring that physical security measures do not breach relevant employer occupational health and safety obligations.

Entity analysis

The PSPF takes into account that there is considerable variation in the size and duties of NCCEs. NCCEs vary in size from micro entities with fewer than 20 staff through to extra-large entities employing over 10,000 staff. Likewise, entities undertake a range of duties, depending on their operational, regulatory, policy and specialist roles. As such, entities engage with and mitigate a wide range of risks in the everyday performance of their duties.

Entities posing a heightened security risk

AGD uses compliance reporting to identify NCCEs that may pose a heightened risk to the government's security posture. If a heightened risk is identified, AGD advises that entity that it potentially poses a heightened risk to the government's security risk posture and offers assistance in addressing issues to increase compliance. The risk posed by an NCCE is assessed against the following criteria:

- does not report (additional criteria element included from the 2016–17 reporting period)
- reports non-compliance with 10 or more PSPF requirements
- has not adopted a risk management approach to security (indicated through non-compliance with mandatory PSPF requirement GOV-6), and/or
- reports a substantive decline in entity compliance (by three or more mandatory requirements).

The 2017–18 reporting period recorded a reduction in the number of NCCEs considered to pose a heightened security risk, with 14 NCCEs identified in 2017–18 (compared to 16 NCCEs in both 2016–17 and 2015–16[4]).

For the entities found to pose a security risk, no more than two risk criteria applied. There were five NCCEs where two risk criteria applied. Of these five:

- two did not achieve full compliance with 10 or more mandatory requirements **and** failed to adopt a risk management approach to security
- two did not achieve full compliance with 10 or more mandatory requirements **and** reported a decline in compliance by three or more requirements, and
- one failed to adopt a risk management approach to security **and** reported a decline in compliance by three or more requirements.

Of the remaining nine NCCEs considered to pose a heightened security risk:

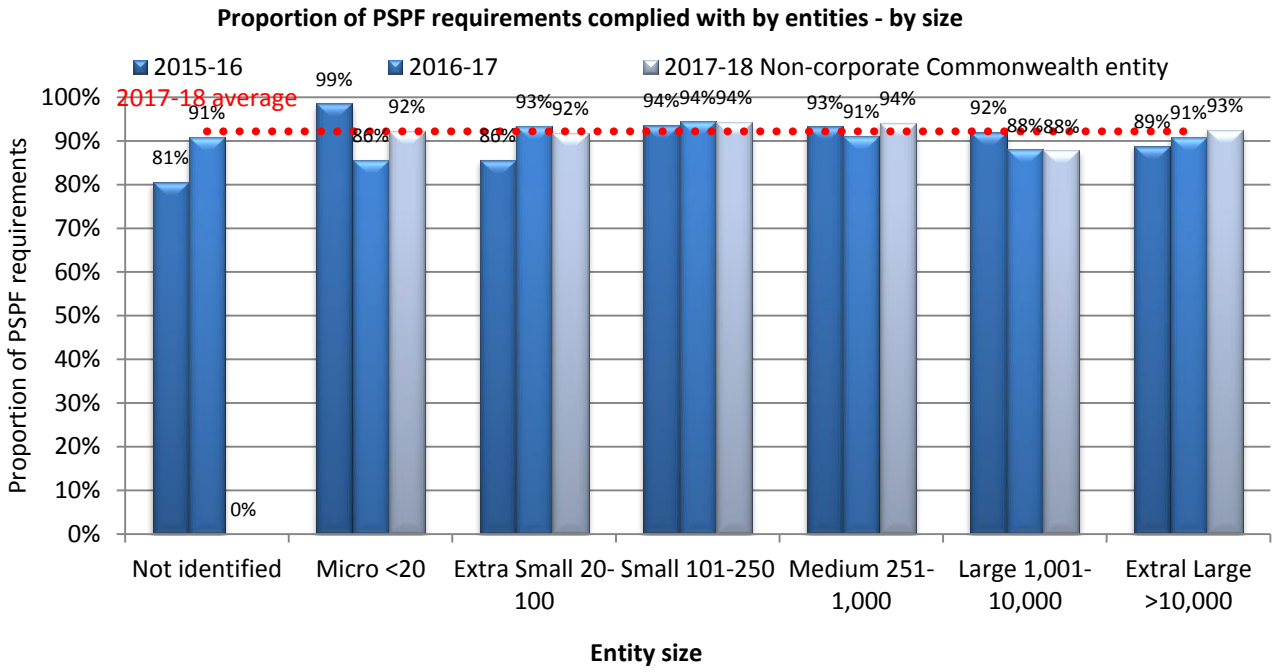
- one identified 10 or more mandatory requirements against which it did not achieve full compliance
- four did not adopt a risk management approach to security, and
- four reported a decline in compliance by three or more requirements.

[4] These figures are based on the four criteria outlined and relate to NCCEs only. Any discrepancies with previously reported data from the reporting period 2015-16 or earlier are the result of the addition of 'does not report' to the criteria for assessing an entity's risk in 2016–17 and separating CCEs and Commonwealth company data from NCCE data from final figures in this report.

Entities demonstrating better-practice: size and function

The Australian Public Service Commission (APSC) groups entities by size and function.[5] In 2017–18, all entities sized from micro to extra-large, excluding large entities, reported average levels of compliance above 91.8% equating to compliance with 33 of the 36 mandatory requirements. Large entities reported average levels of compliance with PSPF requirements of 87.8% equating to 31.6 of the 36 PSPF requirements. This represented a very marginal decline (0.25%) in compliance for large entities from the 2016–17 reporting period.

Figure 7: Proportion of PSPF requirements that NCCEs complied with by entity size



Consistent with 2016–17 results, regulatory and specialist NCCEs reported higher average levels of compliance with PSPF requirements than other entity types with:

- Regulatory entities reporting compliance with 94.91% of the PSPF requirements (34.2 of the 36 mandatory requirements).
- Specialist NCCEs reporting a level of compliance of 91.93% with PSPF requirements (33.1 of the 36 mandatory requirements) and 45.24% of specialist NCCEs reported full compliance with all PSPF requirements, the highest proportion of any entity type when measured according to function.

[5] Entity function types are: policy, specialist, regulatory, smaller operational and larger operational. Entity sizes are: micro (<20 staff), extra-small (20–100 staff), small (101–250), medium (251–1,000), large (1,001–10,000) and extra-large (>10,000).

Corporate Commonwealth Entities: Compliance Summary

Eight CCEs submitted a PSPF compliance report in 2017–18. Noting the very small sample size, as well as the fact that reporting is optional for CCEs and CCs, it is not possible to draw any meaningful trends from the compliance data. Two CCEs reported full compliance with all 36 PSPF requirements and two CCEs reported no non-compliance against any of the 36 PSPF requirements in 2017–18.[6] CCEs reported:

- full compliance with all physical security requirements
- almost full compliance with all personnel security requirements. Across the eight reporting CCEs, there was one citizenship waiver which was held at the Baseline level
- high levels of compliance with security governance requirements—on average the eight CCEs complied with 12 of the 13 governance security requirements (92.31%)
- compliance with 6.5 of the 7 information security requirements (92.86%).

[6] Entities may report policy exceptions that may preclude certain PSPF requirements from applying to the reporting entity. In those cases entities cannot report full compliance, but can report no non-compliance.

Attachment A: 2017–18 Summary NCCE compliance data and variances from 2016–17 for 36 PSPF requirements

PSPF Requirements		Number of fully compliant NCCEs (n=94)	Percentage of NCCEs fully compliant		Percentage point variance	**Comment** [N/A = variance is 5 percentage points or fewer and is not considered significant]
		2017–18	2017–18 (n=94)	2016–17 (n=93)		
Security 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.	85	90.4%	88.2%	+2.2	N/A
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.	94	100.0%	97.8%	+2.2	N/A
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.	92	97.9%	96.8%	+1.1	N/A
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.	79	84.0%	79.6%	+4.4	N/A
GOV-5	Entities must develop their own set of protective security policies and procedures to meet their specific business needs.	83	88.3%	84.9%	+3.4	N/A
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*.	87	92.6%	91.4%	+1.2	N/A
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. *(continued over page)*	94	100.0%	100.0%	±0.0	No change in compliance

PSPF Requirements		Number of fully compliant NCCEs (n=94)	Percentage of NCCEs fully compliant		Percentage point variance	Comment [N/A = variance is 5 percentage points or fewer and is not considered significant]
		2017–18	2017–18 (n=94)	2016–17 (n=93)		
	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*.	91 (excl. 2 N/A)	96.8%	93.5%	+3.3	N/A
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.	91	96.8%	96.8%	±0.0	No change in compliance
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.	81 (excl. 10 N/A)	86.2%	86.0%	+0.2	N/A
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.	90	95.7%	90.3%	+5.4	7 of the 9 non-compliant entities in 2016-17 implemented BCM programs in accordance with their implementation strategy in the 2017-18 period
GOV-12	Entities must ensure the contracted service provider complies with the requirements of this policy and any protective security protocols.	91	94.7%	93.5%	+1.1	N/A
GOV-13	Entities must comply with section 10 of the *Public Governance, Performance and Accountability Rule 2014* and the *Commonwealth Fraud Control Policy*.	94	100.0%	98.9%	+1.1	N/A
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.	88	93.6%	91.4%	+2.2	N/A
PERSEC-2	Entities must have policies and procedures to assess and manage the ongoing suitability for employment of their personnel.	85	90.4%	88.2%	+2.2	N/A
PERSEC-3	Entities must identify, record and review positions that require a security clearance and the level of clearance required.	91 (excl. 1 N/A)	96.8%	94.6%	+2.2	N/A

PSPF Requirements		Number of fully compliant NCCEs (n=94)	Percentage of NCCEs fully compliant		Percentage point variance	**Comment** [N/A = variance is 5 percentage points or fewer and is not considered significant]
		2017–18	2017–18 (n=94)	2016–17 (n=93)		
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.	85 (excl. 3 N/A)	90.4%	93.5%	-3.1	N/A
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.	87 (excl. 5 N/A)	92.6%	90.3%	+2.3	N/A
PERSEC-6	Entities, other than authorised vetting entities, must use the Australian Government Security Vetting Entity (AGSVA) to conduct initial vetting and reviews.	93 (excl. 1 N/A)	98.9%	97.8%	+1.1	N/A
PERSEC-7	Entities must establish, implement and maintain security clearance policies and procedures for clearance maintenance in their entities.	84 (excl. 1 N/A)	89.4%	88.2%	+1.2	N/A
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.	91 (excl. 1 N/A)	96.8%	95.7%	+1.1	N/A
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	90 (excl. 1 N/A)	96.8%	92.5%	+4.3	N/A
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.	88	93.6%	91.4%	+2.2	N/A
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.	88 (excl. 1 N/A)	93.6%	94.6%	-1.0	N/A
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.	78 (excl. 2 N/A)	83.0%	88.2%	-5.2	Variation due to entities having identified gaps or changes in their information platforms (for eg, windows tablets with voice and video conferencing capabilities). NCCES noted that they were taking steps to mitigate the risk.

PSPF Requirements		Number of fully compliant NCCEs (n=94)	Percentage of NCCEs fully compliant		Percentage point variance	**Comment** [N/A = variance is 5 percentage points or fewer and is not considered significant]
		2017–18	2017–18 (n=94)	2016–17 (n=93)		
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 Incidents' as detailed in the Australian Government Information Security Manual.	58	61.7%	60.2%	+1.5	N/A
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.	79	84.0%	81.7%	+2.3	N/A
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.	81 (excl. 1 N/A)	86.2%	87.1%	-0.9	N/A
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.	89	94.7%	95.7%	-1.0	N/A
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.	82	87.2%	86.0%	+1.2	N/A
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.	90	95.7%	92.5%	+3.2	N/A
PHYSEC-3	Entities must ensure they fully integrate protective security early in the process of planning, selecting, designing and modifying their facilities.	87 (excl. 1 N/A)	92.6%	94.6%	-2.0	N/A
PHYSEC-4	Entities must ensure that any proposed physical security measure or activity does not breach relevant employer occupational health and safety obligations.	93	98.9%	100.0%	-1.1	N/A

PSPF Requirements		Number of fully compliant NCCEs (n=94)	Percentage of NCCEs fully compliant		Percentage point variance	**Comment** [N/A = variance is 5 percentage points or fewer and is not considered significant]
		2017–18	2017–18 (n=94)	2016–17 (n=93)		
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.	91 (excl. 2 N/A)	96.8%	97.8%	-1.0	N/A
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.	90	95.7%	94.6%	+1.1	N/A
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.	80	85.1%	88.2%	-3.1	N/A