



Australian Government  
Attorney-General's Department

**Protective Security Policy Framework:  
2016-17 Compliance Report**  
Attorney-General's Department

## Protective Security Policy Framework

Effective protective security is essential to the secure delivery of government business.

Security arrangements support government entities to identify threats and manage risks that have the potential to:

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

The Protective Security Policy Framework (PSPF) is administered by the Attorney-General's Department (AGD). It mandates 36 security requirements as detailed at **Attachment A**.

The PSPF applies to non-corporate Commonwealth entities (NCCes) subject to the *Public Governance, Performance and Accountability Act 2013* in 2016–17. For corporate Commonwealth entities and wholly-owned Commonwealth companies (CCEs), the PSPF represents better practice.

Entities are required to undertake an annual self-assessment of their PSPF compliance, then report on their security posture and measures taken to address identified key risks.

### Entity reporting

All NCCes submitted a PSPF compliance report for 2016–17; this is an improvement from 2015–16 where two NCCes failed to report. In addition, five CCEs reported voluntarily (down from 12 in 2015–16).

## Key findings

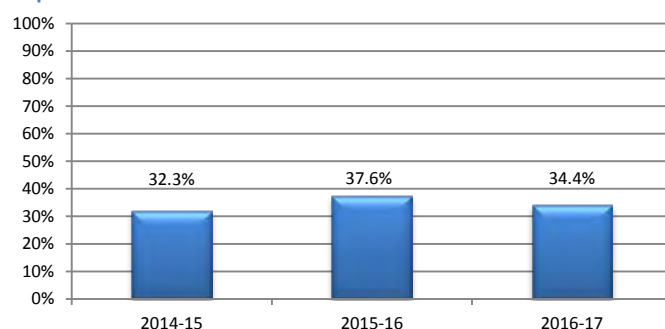
### PSPF compliance

While few (34.4%, 32 entities) NCCes are fully compliant with all of the PSPF, the government's security posture is still broadly sound. On average, NCCes fully comply with a significant proportion of requirements (91.2%, 33 out of 36 – shown as “2016–17 PSPF compliance average” in Figures 3, 4 and 5).

### Key risk areas

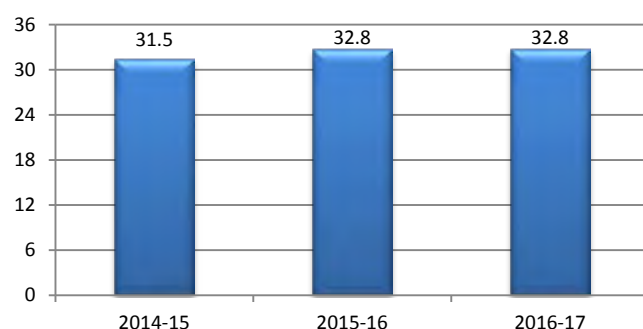
NCCes continue to face challenges in achieving the PSPF's information security requirements. Of note, only 60.2% of NCCes reported full compliance with the INFOSEC 4 requirement.

**Figure 1 Proportion of NCCes fully compliant with all PSPF requirements**



In 2016–17, the proportion of NCCes reporting full compliance with all PSPF mandatory requirements was 34.4%, down from 37.6% in 2015–16 (but up from 32.3% in 2014–15).

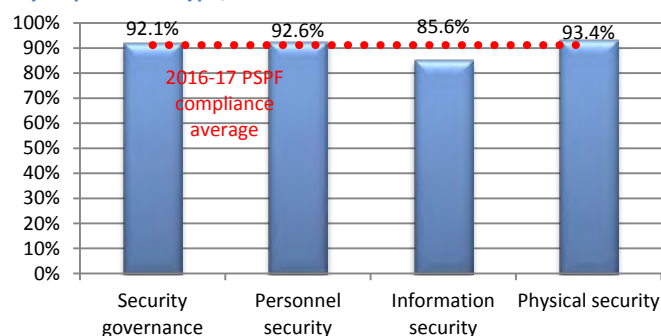
**Figure 2 Average number of PSPF requirements that NCCes complied with**



On average NCCes fully complied with 91.2% of the PSPF's requirements, this is equivalent to 33 out of 36 PSPF requirements. The number of requirements entities comply with has remained broadly stable over time, being:

- 33 out of 36 requirements, 91.0%, in 2015–16 and
- 32 requirements, 87.5% in 2014–15.

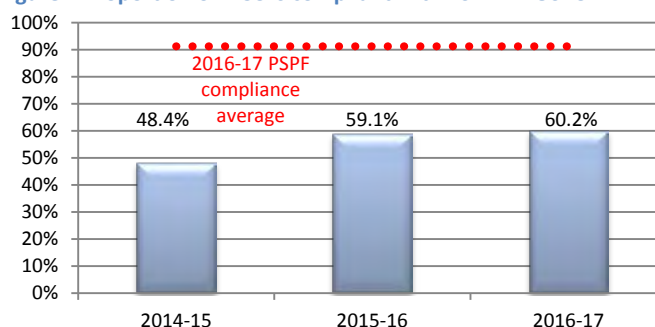
**Figure 3 Proportion of PSPF requirements that NCCes complied with – by requirement type, 2016-17**



Of the PSPF's 36 requirements:

- 13 requirements relate to security governance. On average entities complied with 12.0 of these (92.1% of governance requirements)
- 9 relate to personnel security. NCCes complied with 8.3 (92.6%)
- information and physical security include 7 requirements each. NCCes complied with 6.0 (85.6%) and 6.5 of these (93.4%) of these respectively.

**Figure 4 Proportion of NCCes compliant with PSPF INFOSEC4**



Implementation of the INFOSEC4 requirement (relating to cyber and ICT system security, including the Australian Signals Directorate's *Strategies to Mitigate Targeted Cyber Intrusions*) has improved, but is still a key challenge.

## Security governance

Compliance with PSPF governance requirements was high and remained relatively stable. On average, entities complied with 11.9 of the 13 governance requirements in 2015–16, increasing marginally to compliance with 12 requirements in 2016–17.

Of note, over 95% of NCCEs reported full compliance with the following PSPF governance requirements:

**Table 1 GOVSEC requirements with high compliance, 2016-17**

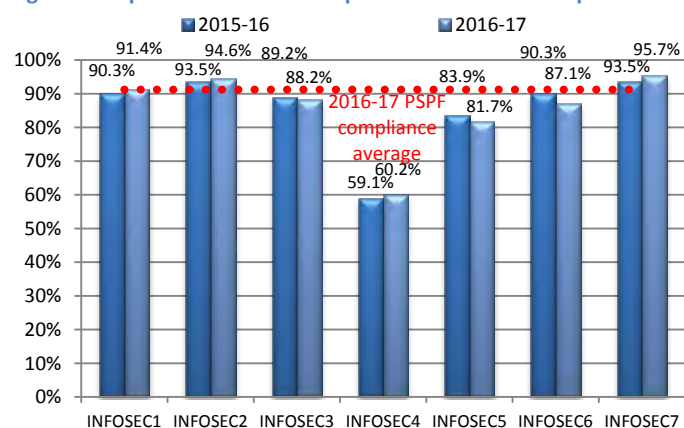
PSPF security governance requirements		Proportion of NCCEs reporting full compliance
<u>GOV-2</u>	Relating to appointment of an entity security executive and supporting advisers	97.8%
<u>GOV-3</u>	Relating to the knowledge and skills of the entity's security staff	96.8%
<u>GOV-7</u>	Relating to annual PSPF compliance reporting	100.0%
<u>GOV-9</u>	Relating to giving employees and contractors guidance on key security-related legislative provisions	96.8%
<u>GOV-13</u>	Relating to fraud control	98.9%

## Information security

Information security is dynamic with challenges posed by continuous technological advancement. Information security arrangements are an important element of an entity's effective protective security regime.

Compliance with information security requirements has been an area of ongoing concern. Despite increased awareness of cyber security risks, and a concerted effort over the year to promote risk mitigation measures,<sup>1</sup> entity compliance with information security requirements did not see significant change. In 2016–17, average compliance remained stable at 6.0 out of 7 requirements.

**Figure 5 Proportion of NCCEs compliant with INFOSEC requirements**



<sup>1</sup> For example, the February 2017 launch of ASD's Essential Eight strategies to mitigate cyber security incidents and the Prime Minister and Cabinet Office of the Cyber Security Special Adviser's ongoing Cyber Security Strategy work.

## Physical security

NCCEs continued to report high-level compliance against the PSPF's physical security requirements. On average NCCEs complied with 6.5 out of 7 requirements, broadly in line with the 2015–16 compliance rate of 6.6.

Of particular note:

- all entities reported full compliance with the PHYSEC 4 requirement to ensure that physical security measures do not breach relevant employer occupational health and safety obligations, and
- almost all entities reported full compliance with the PHYSEC 5 requirement to show a duty of care for the physical safety of members of the public interacting directly with the Australian Government.

A 5.4 percentage point decline in compliance with the PHYSEC 7 requirement was recorded such that ten NCCEs reported they did not have up-to-date plans and/or procedures in place to respond to heightened security levels in case of an emergency or increased threat. Most of these entities reported they expect this matter to be resolved in 2017–18.

## Personnel security

In 2016–17, AGD led outreach activities on security culture and managing the ongoing suitability of personnel.

In line with this, there was a significant (5.4 percentage point) improvement in entities reporting full compliance with the PERSEC2 requirement over the year. Reported compliance has increased from 78.5% of NCCEs in 2014–15 (82.8% in 2015–16) to 88.2% in 2016–17.

PERSEC2 requires entities 'have policies and procedures to assess and manage the ongoing suitability for employment of their personnel'.

Compliance against other personnel security requirements did not see significant change. Average compliance remained stable at 8.3 out of 9 personnel security requirements.

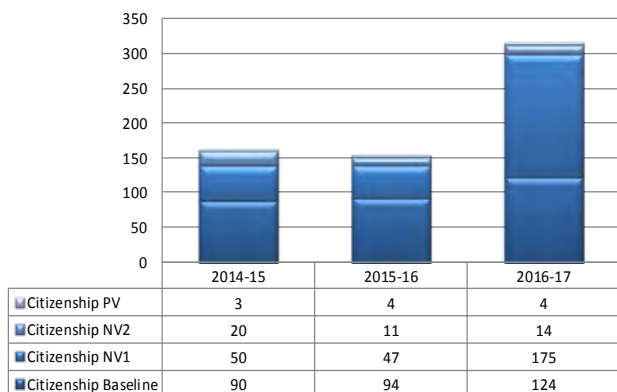
## Personnel security waivers

Access to classified resources is subject to personnel successfully undergoing a vetting process and holding a valid security clearance. Where clearance requirements are waived, government faces increased malicious insider risks (and may be more vulnerable to exploitation from organised crime and interference from foreign governments). There are two types of waivers: waivers of the Australian citizenship requirement, and waivers of the checkable background requirement.

## Waivers of the Australian citizenship requirement

In 2016–17, there were 317 Australian Government security clearance holders who were not Australian citizens. Nonetheless, clearances with a citizenship waiver still make up less than 0.2% of the 200,000+ (as at August 2017) active clearances.

**Figure 6 Number of clearances with a citizenship waiver**



There was a doubling of the number of security clearances with a citizenship waiver over the year (317 in 2016–17, up from 156 in 2015–16). Much of this increase can be attributed to a single entity.

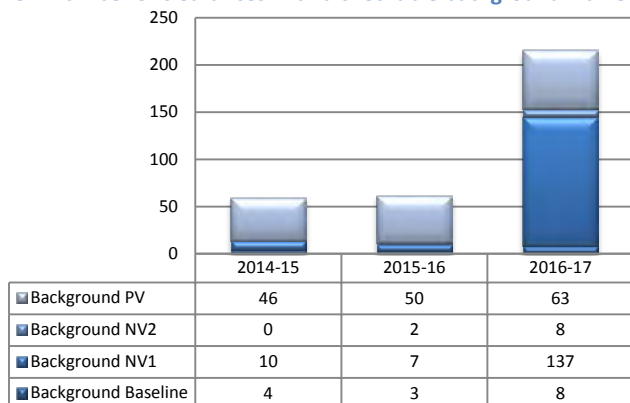
Across government, citizenship waivers at the NV1 level saw the greatest increase over the year (47 in 2015–16, compared with 175 in 2016–17).

## Waivers of checkable background requirement

Assurance about a person's background gives confidence that they can be trusted to protect government information and resources. 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 2016–17, there were 216 people with a security clearance whose background could not be adequately checked. Clearances with checkable background waivers represent only 0.1% of all active clearances.

**Figure 7 Number of clearances with a checkable background waiver**



There was a 248.4% increase in the number of checkable background waivers (from 62 in 2015–16 up to 216 in 2016–17). Much of this can be attributed to a single entity adjusting its reporting methodology over the year. This was not the entity largely responsible for the increase in citizenship waivers.

Historically, checkable background waivers have most commonly been for clearances at the Positive Vetting (PV) level. This reflects more onerous PV background checking expectations.<sup>2</sup> In 2016–17 there were 130 additional NV1 checkable background waivers (from 7 in 2015–16, up to 137). The sizeable increases in checkable background waivers are attributable to a single entity.

## Entity analysis

### Entities posing a heightened security risk

AGD uses compliance reporting to identify NCCs that may pose a heightened risk to the government's security posture. An entity is considered at risk if it:

- does not report
- reports there were 10 or more PSPF requirements against which it did not achieve full compliance
- has not adopted a risk management approach to security (non-compliance with GOV-6), and/or
- reports a substantive decline in entity compliance (by three or more mandatory requirements).

Fewer NCCs were considered at risk, down from 21 in 2015–16 to 16 in 2016–17). Of these entities:

- five NCCs were considered at risk against two or more risk criterion
- a further:
  - four NCCs did not adopt a risk management approach to security
  - one entity identified 10 or more mandatory requirements against which it did not achieve full compliance, and
  - five NCCs reported a decline in compliance by three or more requirements.<sup>3</sup>

### Entities demonstrating better-practice

The Australian Public Service Commission (APSC) groups entities by size and function<sup>4</sup>. In 2016–17:

- the entity function types more likely to report full compliance against requirements were specialist and smaller operational entities, and
- the entity sizes most likely to report compliance against all PSPF requirements were micro, extra small and small entities (up to 250 people).

<sup>2</sup> The 12 month threshold means no more than 10% of a person's background can be uncheckable at the NV2 level without a waiver and the threshold for PV level could be significantly higher, compared to 20% of a person's background at the Baseline level.

<sup>3</sup> During the year, the Joint Committee of Public Accounts and Audit questioned the accuracy of the PSPF's self-assessed compliance reporting, AGD notes a number of these at risk entities had independent reviews to inform their 2016–17 PSPF compliance reports.

<sup>4</sup> Policy, Specialist, Regulatory, Operational (larger and smaller).

## CCE compliance summary

Five CCEs submitted a PSPF compliance report in 2016–17 (down from 12 in 2015–16). Noting the very small sample size, significant variations in year-to-year reported compliance can be expected.

Two CCEs (40%) claimed full compliance with all 36 mandatory requirements, above the NCCE average of 35.5% (33 entities) but well below the 58% of CCEs (7 of 12) reporting full compliance in 2015–16.

On average, CCEs reported full compliance with 35 of the 36 mandatory requirements; this is a slight improvement from the 34.4 compliance average reported in 2015–16 (and above the 32.8 NCCE average). CCEs reported:

- full compliance with all PERSEC requirements. There was one citizenship waiver, held at the Baseline level, across all five entities
- full compliance with all PHYSEC mandatory requirements (an increase from 6.9 of 7 requirements in 2015–16)
- high rates of compliance with GOVSEC mandatory requirements. On average, CCEs complied with 12.4 of 13 requirements (95.4%) in both 2015–16 and 2016–17 (slightly above NCCE average of 12), and
- like NCCEs, compliance was lowest in relation to INFOSEC requirements. CCEs reported compliance with 6.6 of 7 requirements in 2016–17 (94.3%), compared to 6.7 out of 7 in 2015–16.

## Next steps: future policy reforms

The PSPF was considered as part of the *Independent Review of Whole-of-Government Internal Regulation* (Belcher Review). In 2017, Secretaries' Board agreed to reform the PSPF in response to the Belcher Review's recommendations with a new framework to commence from 1 October 2018.

Of note, the current 36 requirements will be consolidated to a set of 16 core requirements.

Additionally, a maturity model will replace current annual PSPF compliance reporting (intended for implementation in 2018–19). While reporting has historically focused on binary indicators of whether an entity is fully compliant with a PSPF requirement (or otherwise), future reporting will be more nuanced towards considering how well entities implement the PSPF in their organisation.<sup>5</sup>

Security maturity reporting aims to capture the level of implementation of an entity's protective security practices to protect its people, information and assets. It provides an assessment of an entity's protective security risk posture as well as its ability to protect government resources and identify key security risks and vulnerabilities.

---

<sup>5</sup> For example, low maturity – where implementation of the PSPF is ad hoc – through to high maturity where security is proactively managed and embedded into entity's business practices in response to the risk environment.

**Attachment A: 2016–17 Summary NCCE compliance data and variances from 2015-16 for 36 PSPF requirements**

PSPF Requirements		No. of total (93) NCCE's fully compliant	% of NCCE's fully compliant		Percentage point variance	Comment [N/A = variance is 5 percentage points or less and is not considered significant]
		2016-17	2016-17	2015-16		
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.	82	88.2%	86.0%	2.2	N/A
GOV-2	To fulfil their security obligations, entities must appoint: <ul style="list-style-type: none"><li>A member of the Senior Executive Service as the security executive, responsible for the entity protective security policy and oversight of protective security practices.</li><li>An entity security adviser (ASA) responsible for the day-to-day performance of protective security functions.</li><li>An information technology security adviser (ITSA) to advise senior management on the security of the entity's Information Communications Technology (ICT) systems.</li></ul>	91	97.8%	97.8%	0.0	No change in compliance
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.	90	96.8%	96.8%	0.0	No change in compliance
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.	74	79.6%	78.5%	1.1	N/A
GOV-5	Entities must develop their own set of protective security policies and procedures to meet their specific business needs.	79	84.9%	84.9%	0.0	No change in compliance
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 <i>Risk management—Principles and guidelines</i> and HB 167:2006 <i>Security risk management</i> .	85	91.4%	90.3%	1.1	N/A
GOV-7	For internal audit and reporting, entities must: <ul style="list-style-type: none"><li>undertake an annual security assessment against the mandatory requirements detailed within the Protective Security Policy Framework</li><li>report their compliance with the mandatory requirements to the relevant portfolio Minister.</li></ul> The report must: <ul style="list-style-type: none"><li>contain a declaration of compliance by the entity head</li><li>state any areas of non-compliance, including details on measures taken to lessen identified risks.</li></ul> In addition to their portfolio Minister, entities	93	100.0%	96.8%	3.2	N/A



PSPF Requirements		No. of total (93) NCCE's fully compliant	% of NCCE's fully compliant		Percentage point variance	Comment [N/A = variance is 5 percentage points or less and is not considered significant]
		2016-17	2016-17	2015-16		
	<p>must send a copy of their annual report on compliance with the mandatory requirements to:</p> <ul style="list-style-type: none"> <li>the Secretary, Attorney-General's Department, and</li> <li>the Auditor General.</li> </ul> <p>Entities must also advise any non-compliance with mandatory requirements to:</p> <ul style="list-style-type: none"> <li>the Director, Australian Signals Directorate for matters relating to the <a href="#">Australian Government Information Security Manual</a> (ISM).</li> <li>the Director-General, Australian Security Intelligence Organisation for matters relating to national security, and</li> <li>the heads of any entities whose people, information or assets may be affected by the non-compliance.</li> </ul>					
<u>GOV-8</u>	<p>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:</p> <ul style="list-style-type: none"> <li><i>Australian Government protective security governance guidelines—Reporting incidents and conducting security investigations</i>, and/or</li> <li><i>Australian Government Investigations Standards</i>.</li> </ul>	87	93.5%	94.6%	-1.1	N/A
<u>GOV-9</u>	<p>Entities must give all employees, including contractors, guidance on Sections 70 and 79 of the <i>Crimes Act 1914</i>, section 91 of the <i>Criminal Code Act 1995</i>, the <i>Freedom of Information Act 1982</i> and the Australian Privacy Principles contained in the <i>Privacy Act 1988</i>, including how this legislation relates to their role.</p>	90	96.8%	94.6%	2.2	N/A
<u>GOV-10</u>	<p>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.</p>	80	86.0%	89.2%	-3.2	N/A
<u>GOV-11</u>	<p>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.</p>	84	90.3%	93.5%	-3.2	N/A
<u>GOV-12</u>	<p>Entities must ensure the contracted service provider complies with the requirements of this policy and any protective security protocols.</p>	87	93.5%	90.3%	3.2	N/A
<u>GOV-13</u>	<p>Entities must comply with section 10 of the <i>Public Governance, Performance and Accountability Rule 2014</i> and the <i>Commonwealth Fraud Control Policy</i>.</p>	92	98.9%	97.8%	1.1	N/A

PSPF Requirements		No. of total (93) NCCE's fully compliant	% of NCCE's fully compliant		Percentage point variance	Comment [N/A = variance is 5 percentage points or less and is not considered significant]
		2016-17	2016-17	2015-16		
Information security						
<u>INFOSEC-1</u>	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.	85	91.4%	90.3%	1.1	N/A
<u>INFOSEC-2</u>	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	94.6%	93.5%	1.1	N/A
<u>INFOSEC-3</u>	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.	82	88.2%	89.2%	-1.1	N/A
<u>INFOSEC-4</u>	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.	56	60.2%	59.1%	1.1	N/A
<u>INFOSEC-5</u>	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.	76	81.7%	83.9%	-2.2	N/A
<u>INFOSEC-6</u>	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	87.1%	90.3%	-3.2	N/A
<u>INFOSEC-7</u>	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	95.7%	93.5%	2.2	N/A
Physical security						
<u>PHYSEC-1</u>	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.	80	86.0%	90.3%	-4.3	N/A



PSPF Requirements		No. of total (93) NCCCE's fully compliant	% of NCCCE's fully compliant		Percentage point variance	Comment [N/A = variance is 5 percentage points or less and is not considered significant]
		2016-17	2016-17	2015-16		
<u>PHYSEC-2</u>	Entities must have in place policies and procedures to: <ul style="list-style-type: none"> <li>• 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</li> <li>• report incidents to management, human resources, security and law enforcement authorities, as appropriate</li> <li>• provide information, training and counselling to employees, and</li> <li>• maintain thorough records and statements on reported incidents.</li> </ul>	86	92.5%	92.5%	0.0	No change in compliance
<u>PHYSEC-3</u>	Entities must ensure they fully integrate protective security early in the process of planning, selecting, designing and modifying their facilities.	88	94.6%	93.5%	1.1	N/A
<u>PHYSEC-4</u>	Entities must ensure that any proposed physical security measure or activity does not breach relevant employer occupational health and safety obligations.	93	100.0%	97.8%	2.2	N/A
<u>PHYSEC-5</u>	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	97.8%	96.8%	1.1	N/A
<u>PHYSEC-6</u>	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.	88	94.6%	93.5%	1.1	N/A
<u>PHYSEC-7</u>	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.	82	88.2%	93.5%	-5.4	Ten NCCCEs reported they did not have up-to-date plans and/or procedures in place to respond to heightened security levels in case of emergency or increased threat. Most of these entities reported they expect this matter to be resolved in 2017-18. One further entity further claimed this requirement was not applicable to their business.

PSPF Requirements		No. of total (93) NCCE's fully compliant	% of NCCE's fully compliant		Percentage point variance	Comment [N/A = variance is 5 percentage points or less and is not considered significant]
		2016-17	2016-17	2015-16		
Personnel security						
<u>PERSEC-1</u>	Entities must ensure that their personnel who access Australian Government resources (people, information and assets): <ul style="list-style-type: none"><li>are eligible to have access</li><li>have had their identity established</li><li>are suitable to have access, and</li><li>agree to comply with the Government's policies, standards, protocols and guidelines that safeguard that entity's resources from harm.</li></ul>	85	91.4%	93.5%	-2.2	N/A
<u>PERSEC-2</u>	Entities must have policies and procedures to assess and manage the ongoing suitability for employment of their personnel.	82	88.2%	82.8%	5.4	AGD led a series of outreach activities with a key focus on security culture and managing the ongoing suitability of personnel. In line with this, there was a significant improvement in entities reporting full compliance.
<u>PERSEC-3</u>	Entities must identify, record and review positions that require a security clearance and the level of clearance required.	88	94.6%	91.4%	3.2	N/A
<u>PERSEC-4</u>	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.	87	93.5%	93.5%	0.0	No change in compliance
<u>PERSEC-5</u>	Before issuing an eligibility waiver (citizenship or checkable background) and prior to requesting an Australian Government security clearance an entity must: <ul style="list-style-type: none"><li>justify an exceptional business requirement</li><li>conduct and document a risk assessment</li><li>define the period covered by the waiver (which cannot be open-ended)</li><li>gain agreement from the clearance applicant to meet the conditions of the waiver</li><li>consult with the vetting entity.</li></ul>	84	90.3%	94.6%	-4.3	N/A
<u>PERSEC-6</u>	Entities, other than authorised vetting entities, must use the Australian Government Security Vetting Entity (AGSVA) to conduct initial vetting and reviews.	91	97.8%	97.8%	0.0	No change in compliance

PSPF Requirements		No. of total (93) NCCE's fully compliant	% of NCCE's fully compliant		Percentage point variance	Comment [N/A = variance is 5 percentage points or less and is not considered significant]
		2016-17	2016-17	2015-16		
<u>PERSEC-7</u>	Entities must establish, implement and maintain security clearance policies and procedures for clearance maintenance in their entities.	82	88.2%	87.1%	1.1	N/A
<u>PERSEC-8</u>	Entities and vetting entities must share information that may impact on an individual's ongoing suitability to hold an Australian Government security clearance.	89	95.7%	95.7%	0.0	No change in compliance
<u>PERSEC-9</u>	Entities must have separation policies and procedures for departing clearance holders, which includes a requirement to: <ul style="list-style-type: none"> <li>inform vetting entities when a clearance holder leaves entity employment or contract engagement</li> <li>advise vetting entities of any security concerns</li> </ul>	86	92.5%	95.7%	-3.2	N/A