Protective Security Policy Framework 2014-15 Compliance Report

Protective Security Policy
Attorney-General’s Department

Protective Security Policy Framework (PSPF)
2014-15 Compliance Report

Protective Security Policy Framework

2014-15 Compliance Report

Report summary

Effective protective security is essential to the secure delivery of government business. Well-designed protective security arrangements support Australian Government agencies[1] to identify threats and manage risks that have the potential to harm staff or members of the public; compromise official information or assets; or interrupt progress toward meeting the government's policy objectives.

This report is the second report to government on the progress of agency compliance with the Australian Government's Protective Security Policy Framework (PSPF) and the first report that will compare compliance levels between years. This report provides an overview of PSPF implementation in 2014-15, highlights significant trends identified by aggregate compliance data, including areas of non-compliance that ~~require additional government efforts to mitigate security risks~~. The report is a component of the Whole of Government Protective Security Status Report (PSSR).

The *Independent Review of Whole-of-Government Internal Regulation*, also known as the 'Belcher Red Tape Review' made a number of recommendations directed to the Attorney-General's Department (AGD) on the PSPF covering personnel security, governance, and information security. AGD supports and has agreed to implement these recommendations.

In August 2015, AGD convened a Personnel Security Strategic Reforms Taskforce which will implement these and other relevant recommendations relating to employment screening and security vetting. The taskforce aims to address ongoing limitations to the Australian Government's personnel security arrangements and introduce reforms to efficiently and effectively mitigate the risk posed by the malicious insider threat. A central element is the consideration of risk factors (attitudes and behaviours) that are inconsistent with community expectations of Australian Government personnel. An example of these risk factors is an individual's associations or links with serious and organised crime.

Key findings

- Broadly, 2014-15 compliance data demonstrates that both the proportion of agencies which are non-compliant with the PSPF and the extent to which agencies are non-compliant has increased since the 2013-14 reporting period.
- Fluctuation in some agencies' compliance levels from compliant in 2013-14 to non-compliant in the 2014-15 reporting period may indicate that successful implementation of the PSPF in one period does not guarantee ongoing success in a changing security environment. Maintaining gains in protective security measures requires ongoing leadership, active management within the agency, agility to adapt to changing threat environments and a strong culture of security.
- Many agencies reported using scalable compliance terminology to more accurately reflect progress toward achieving compliance with the PSPF. For example, reporting as partially compliant or substantially compliant against a mandatory requirement is reflected in this report as non-compliance to allow comparison between agencies. As a result, there is potentially a lower level of non-compliance in practice.
- ~~Agency reporting in 2014-15 indicates that information security is an ongoing challenge for the Australian Government and for a large number of agencies which have been unable to fully implement the Australian~~

[1] In this report, 'Agency' or 'Agencies' refers to all non-corporate Commonwealth entities (NCCE) and any corporate Commonwealth entities (CCE) that have nominated to report compliance against the PSPF.

~~Signals Directorate's (ASD) 'Top 4 Controls' to mitigate cyber intrusion. Information security represents an area of escalating risk for the Australian Government.~~

Background

The PSPF forms the basis of the government's protective security measures that facilitates trust and confidence in and between agencies to support the secure and efficient delivery of government business. The PSPF provides appropriate controls for the Australian Government to protect its people, information and assets, at home and overseas. Introduced in 2010, the PSPF represents a significant departure from the 'one size fits all' compliance approach taken by its predecessor, the Protective Security Manual (PSM). The PSPF identifies 36[2] mandatory requirements to safeguard the Australian Government's personnel, information and assets.

The PSPF enables agencies to take a risk-based approach to protective security based on individual business needs. Considering the PSPF applies to 96[3] agencies, from national security agencies, museums, media and health authorities, the PSPF allows greater flexibility for agencies to apply security risk mitigation strategies proportionate to their threat environment. The PSPF is a responsive framework that enables each agency to respond to the unique challenges of its operating environment, while ensuring a consistent approach to the secure delivery of government business and protection of the national interest. It supports improved information sharing across agencies and governments (state, territory, Commonwealth) and provides assurance and trust to support engagement with the private sector.

The Attorney-General, as the responsible minister, has given the directive for agency heads to have in place effective protective security arrangements. Annual compliance reports from agencies allow AGD on behalf of the Attorney-General to assess:

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

Agency reporting

Agencies[4] are required to report their compliance with the PSPF to their Minister, the Secretary of AGD and the Australian National Audit Office (ANAO) on an annual basis. Financial year 2013-14 was the first time that annual compliance reporting via a template approach came into effect. A total of 103 agencies reported their compliance against the PSPF in 2014-15. This included 94 non-corporate Commonwealth entities (NCCEs), eight corporate Commonwealth entities (CCEs) and one Royal Commission[5] (RC).

[2] This is an increase from 33 mandatory requirements reported in 2013-14. Three additional personnel security requirements were introduced in September 2014, making a total of 36 mandatory requirements.

[3] As at August 2015 there were 96 non-corporate Commonwealth entities (NCCE). Only 94 agencies reported against the PSPF for this period as one agency was newly established in July 2015, one agency had been abolished during the period, one agency was exempted from reporting and the Australian Customs and Border Protection Service reported separately from Department of Immigration and Border Protection.

[4] Non-corporate Commonwealth entities (NCCEs) *(*under the *Public Governance, Performance and Accountability Act 2013* as of 1 July 2014) are required to report their compliance with the PSPF. Corporate Commonwealth entities (CCEs) and Commonwealth companies (CCs) are not required to apply policies of the Australian Government.

CCEs are not required to implement or report against the PSPF, however a number have either been directed by their Minister or chosen to report on their compliance level against the PSPF in 2014-15. This will provide important baseline data to inform future reporting when the proposed Government Policy Order (GPO) is introduced. The GPO will extend some of the key requirements of the PSPF to all CCEs and Commonwealth Companies (see *Next Steps*, page 10).

Compliance reporting relies on the accuracy of captured data and assumes that agencies have sufficiently robust systems to record evidence of compliance or non-compliance. ANAO reports suggest there may be issues with the accuracy and quality of the data provided by compliance reporting, due to the self-reporting nature of the process. Previous ANAO audits identified that some agencies did not have sufficient evidence to support their statements of compliance (*Cyber Attacks: Securing Agencies' ICT Systems* and *The Management of Physical Security*). To address this concern, agencies are encouraged to have their compliance reports audited, either independently or through internal audit functions.

Responses to the PSPF Compliance Report 2013-14 and 2014-15

Reporting Period	2013-14	2014-15
Non-corporate Commonwealth Entities (NCCE)	104	95
NCCEs exempted from reporting	0	1
Corporate Commonwealth Entities (CCE)	8	8
Royal Commissions (RC)	1	1
Total compliance data	**113**	**103**

2014-15 findings

Of the 103 compliance reports received by AGD, 30 agencies reported full compliance and 73 agencies self-assessed as non-compliant with at least one mandatory requirement of the PSPF. Of the 73 non-compliant agencies, one agency reported non-compliance due to a conflict between a PSPF requirement and core business needs. Consistent with a risk-based approach, some agencies who reported non-compliance also indicated they were actively engaging with the risks associated with their non-compliance. In the majority of these cases, agencies either had mitigation measures in place or were taking direct action to achieve compliance in the near future, taking into account planning and resourcing requirements.

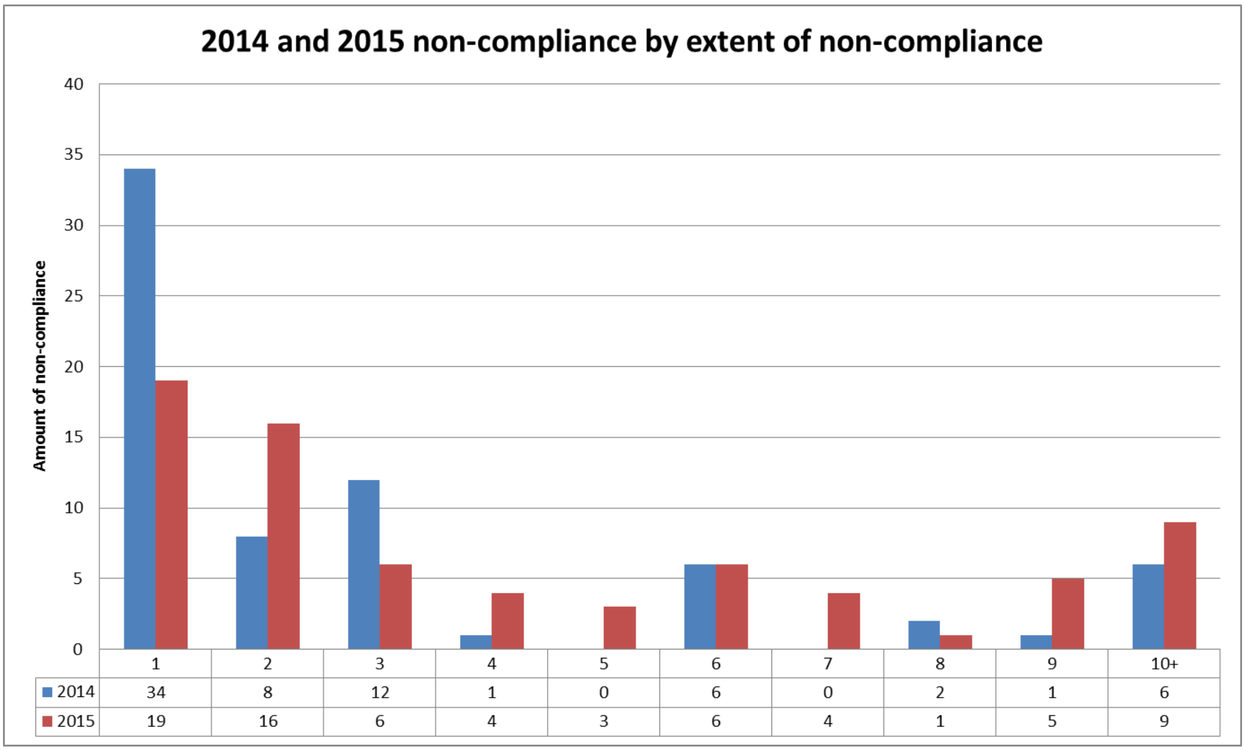
Information security continues to represent the highest level of non-compliance, with agencies still finding it challenging to implement ASD's 'Top 4 Strategies' for mitigating cyber intrusions. Information security is an area of ongoing risk for the Australian Government (see *Figure 2* and page 9 for further detail).

Overall levels of compliance have declined from 36 per cent compliance in financial year 2013-14 to 29 per cent in 2014-15. This report is the first time agencies have been required to assess compliance against three new personnel security requirements introduced in 2014. The introduction of the new requirements during this reporting period has not significantly contributed to the overall increase in non-compliance in 2014-15, with only one agency attributing its non-compliance in 2014-15 solely to the new requirements.

In 2014-15, 56 per cent of non-compliant agencies reported non-compliance with between one and three requirements, and 44 per cent of agencies reported non-compliance with between four and 16 mandatory requirements. This is a significant increase from 2013-14, with only 22.9 per cent of agencies reporting non-

[5] Royal Commissions come under the portfolio of the Attorney-General's Department; however, one Royal Commission maintains an independent administration and manages information separately from the department. Based on this arrangement, the Commission has nominated to provide a separate report on their level of compliance.

compliance with more than three requirements. This demonstrates that not only is the proportion of agencies which are non-compliant with the PSPF increasing; the extent of the non-compliance has also increased between reporting periods. The extent of non-compliance between 2013-14 and 2014-15 is represented in *Figure 1.*



	1	2	3	4	5	6	7	8	9	10+
🟦 2014	34	8	12	1	0	6	0	2	1	6
🟥 2015	19	16	6	4	3	6	4	1	5	9

Figure 1: 2013-14 and 2014-15 comparison by extent of non-compliance

The data collected in 2014-15 shows fluctuation in agency compliance, in some cases from compliant in 2013-14 to non-compliant in 2014-15. Of the 40 agencies that reported full compliance in 2013-14, 50 per cent of these agencies reported non-compliance in 2014-15. This may indicate that maintaining full compliance with the PSPF requires separate measures to sustain gains and allow continuous improvement. Erosion of compliance levels could suggest that the initial effort to implement the PSPF has not been sustained through a change in security culture at the organisational level or the ability to adapt to changing threat environments. Changes in the security environment, for example through the introduction of heightened security alert levels in September 2014, may have contributed to the decline in agencies' compliance.

Fluctuations in compliance could also reflect a maturing of agencies' risk management skills and the ability to self-assess implementation of the PSPF. This may be a result of improved processes and increasingly robust systems which increases awareness of an agency's compliance level.

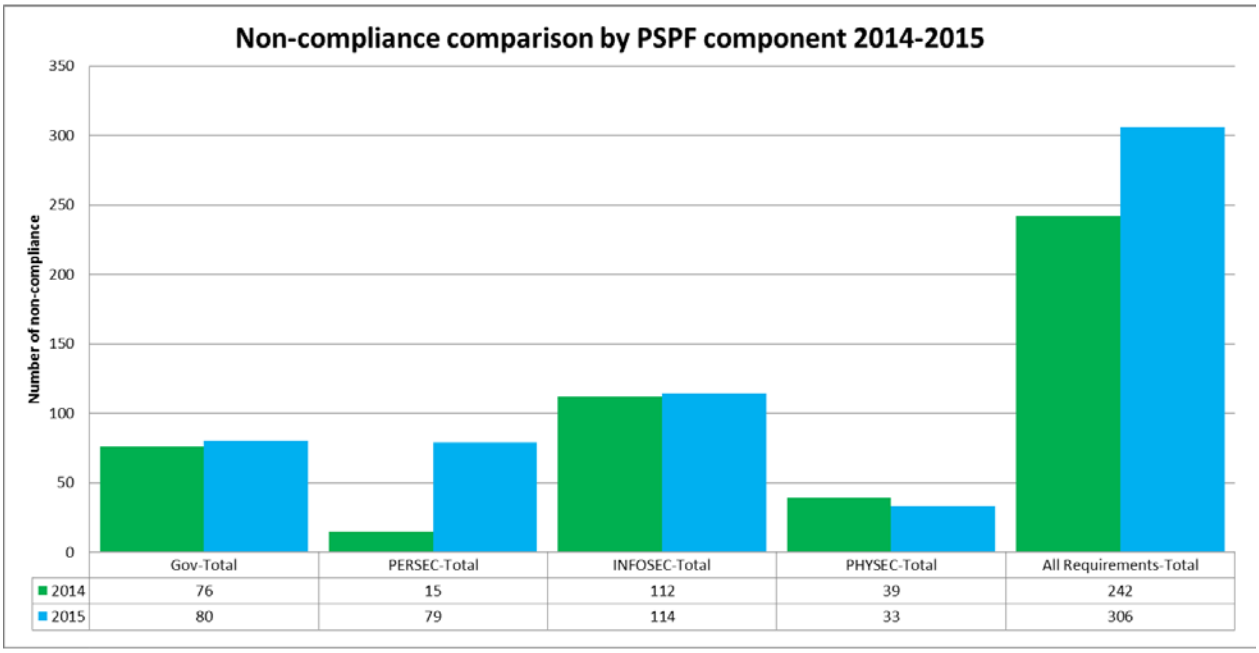
The current method of compliance reporting allow agencies to report only as non-compliant or compliant and is unable to reflect partial compliance or improvements with a requirement. A number of agencies reported in 2014-15 using scalable compliance terminology to reflect incremental progress toward achieving compliance with some aspects of the PSPF. These agencies reflect their trajectory in implementing the PSPF using terminology such as; compliant, substantially compliant, partially compliant and non-compliant. Some agencies apply thresholds to compliance reporting, for example, an agency might consider itself compliant if it is 80 per cent compliant with a requirement, whereas another agency may require 100 per cent compliance before reporting as compliant against the same requirement. This can lead to inconsistent reporting of compliance levels.

Of the 72 agencies that self-assessed as non-compliant in 2013-14, 13 agencies reported full compliance in 2014-15 demonstrating a marked commitment to improving protective security measures. A further 12 agencies reported increasing compliance with the requirements but remained non-compliant overall. Twenty-one agencies' compliance further deteriorated and 13 reported no change from the 2013-14 compliance levels. No compliance data is available for the remaining agencies.[6]

Twenty-nine agencies were assessed to be at risk based on 2013-14 compliance reporting. Agencies were assessed according to three criteria; non-compliance with 10 or more mandatory requirements, non-compliance with the requirement to adopt a risk management approach (GOV-6) and agencies with no improvement compared with the previous year. Over the following 12 months, AGD communicated directly with the agencies to offer additional support in applying the PSPF. The 2014-15 data shows that on average, the compliance level of these agencies improved, with five agencies reporting full compliance and another eight agencies showing improvement on the 2013-14 level of compliance. Six agencies reported the same level of non-compliance as the previous year and another six agencies further declined in their levels of compliance. No compliance data is available for the final four agencies.[7]

According to 2014-15 compliance data, a total of 26 agencies were assessed to be at risk. Agencies were assessed to be at risk according to 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 agency compliance by three or more mandatory requirements. AGD is considering a range of outreach and educational activities in the next twelve months to further support agencies considered to be at risk following 2014-15 reporting. This support will also aim to improve understanding of the threat environment and agency risk appetite in applying the PSPF.

Compliance against the PSPF components



	Gov-Total	PERSEC-Total	INFOSEC-Total	PHYSEC-Total	All Requirements-Total
🟩 2014	76	15	112	39	242
🟦 2015	80	79	114	33	306

Figure 2: Comparison of agencies' non-compliance between Governance, Personnel Security, Information Security, and Physical Security Mandatory Requirements

[6] Due to a combination of exemption to the PSPF, agencies reporting as part of another entity due to machinery of government changes and no response from some CCEs in 2015.

[7] Due to a combination of exemption to the PSPF and no response from CCEs. Note that the 2013-14 report listed 30 agencies being non-compliant in error.

Governance (GOV)

Strong governance arrangements and practices are critical to achieving protective security through providing appropriate oversight and management of risks and security arrangements. In 2014-15, the governance component of the PSPF has the second highest level of non-compliance of any PSPF component.

Risk management approach

The varied and unique operating environment of government requires an agile and flexible approach to protective security that engages with risk and fosters innovation, leading to an increase in productivity of government business. A proportionate risk-based approach to security is a flexible, yet structured approach to managing the security of an entity based on individual context and risk tolerance. Adopting a risk-based approach is fundamental to creating a culture of security, in which improvements in protective security measures and attitudes eventually become self-sustaining. Based on 2014-15 compliance reporting, AGD has assessed that not all agencies have consistently adopted a risk-based approach to protective security.

GOV-6 - Agencies must adopt a risk management approach to cover all areas of protective security activity across their organisation, in accordance with the Australian Standards AS/NZS ISO 31000:2009 Risk management—Principles and guidelines and HB 167:2006 Security risk management.

The PSPF is underpinned by a risk management approach to protective security (GOV-6). This approach allows agencies to implement the PSPF in a way that is proportionate and relevant to their operating environment. An in depth understanding of the risk profile and specific threats allow agencies to apply the PSPF appropriate to their business requirements. When implemented in accordance with international standard (AS/NZS ISO31000), by applying appropriate and targeted risk mitigation strategies, the risk-based approach to protective security can create efficiencies and ensure that agency efforts are directed at the areas of greatest risk. Agencies reporting non-compliance against GOV-6 (10 agencies in 2014-15) demonstrate an inadequate understanding of their risk environment and how the PSPF enables the secure delivery of their business. This is a reduction from 13 agencies reporting non-compliance with GOV-6 in 2013-14.

(s 47E) [redacted]

[redacted]

[redacted].

(s 47E) [redacted]

[redacted]

[redacted]

Personnel security (PERSEC)

Personnel security arrangements provide agencies with a level of assurance as to the eligibility and suitability of its personnel to access Australian Government resources. In 2014-15, personnel security has the third highest level of non-compliance.

To meet evolving threats and in the wake of high profile trusted insider incidents, the Attorney-General launched the first tranche of changes to strengthen the government's personnel security policy in October 2014. The original six personnel security mandatory requirements were increased to nine (taking the total number of mandatory requirements to 36). These changes were made to:

- reduce the risk of loss, damage or compromise of Australian Government resources by providing assurance about the suitability of personnel authorised to access those resources
- create an environment where those accessing Australian Government resources are aware of the responsibilities that come with that access and uphold their obligations
- minimise potential for misuse of Australian Government resources through inadvertent or deliberate unauthorised disclosure, and.
- support a culture of protective security.

In 2014-15, a total of 23 agencies reported non-compliance with one or more of the three new PERSEC requirements. Further reforms are being considered by the Personnel Security Strategic Reforms Taskforce. The reforms aim to efficiently direct resources to individuals of greatest risk through improved information sharing, and the use of assurance ratings and automated continuous assessments.

The backlog in security clearance revalidations represents a (s 33) [redacted] trusted insider risk for the Australian Government. As at 19 October 2015, there were over (s 33) [redacted] security clearances overdue for revalidation, with a further (s 33) [redacted] clearances becoming overdue in 2016.[8] These personnel potentially have access to classified

[8] As reported by the Australian Government Security Vetting Agency (AGSVA). This includes overdue revalidations for clearances at the Entry, Restricted, Confidential, Protected and Highly Protected levels, as well as Baseline, negative vetting and positive vetting. AGSVA has provided data on overdue revalidations by adding the appropriate revalidation period (for

information, some at the most sensitive levels, and in some cases their suitability to hold a clearance has not been reviewed in over a decade.

Eligibility waivers

PERSEC-5 states that an agency head may, in exceptional circumstances and after conducting a thorough risk assessment, waive citizenship or checkable background requirements applicable for an Australian Government security clearance. Clearances issued with citizenship or checkable background waivers must be role specific, time-limited, subject to review and not portable between agencies.

Eligibility waivers in Australian Government security clearances represent a vulnerability to exploitation from organised crime and foreign governments. It is the responsibility of each agency to consider the need for waivers on an ongoing basis. Agencies reported 177 eligibility waivers held in 2014-15, compared to a reported 270 waivers held in 2013-14, equating to a 34% decline in waivers held from 2014-15 to 2013-14.

Information security (INFOSEC)

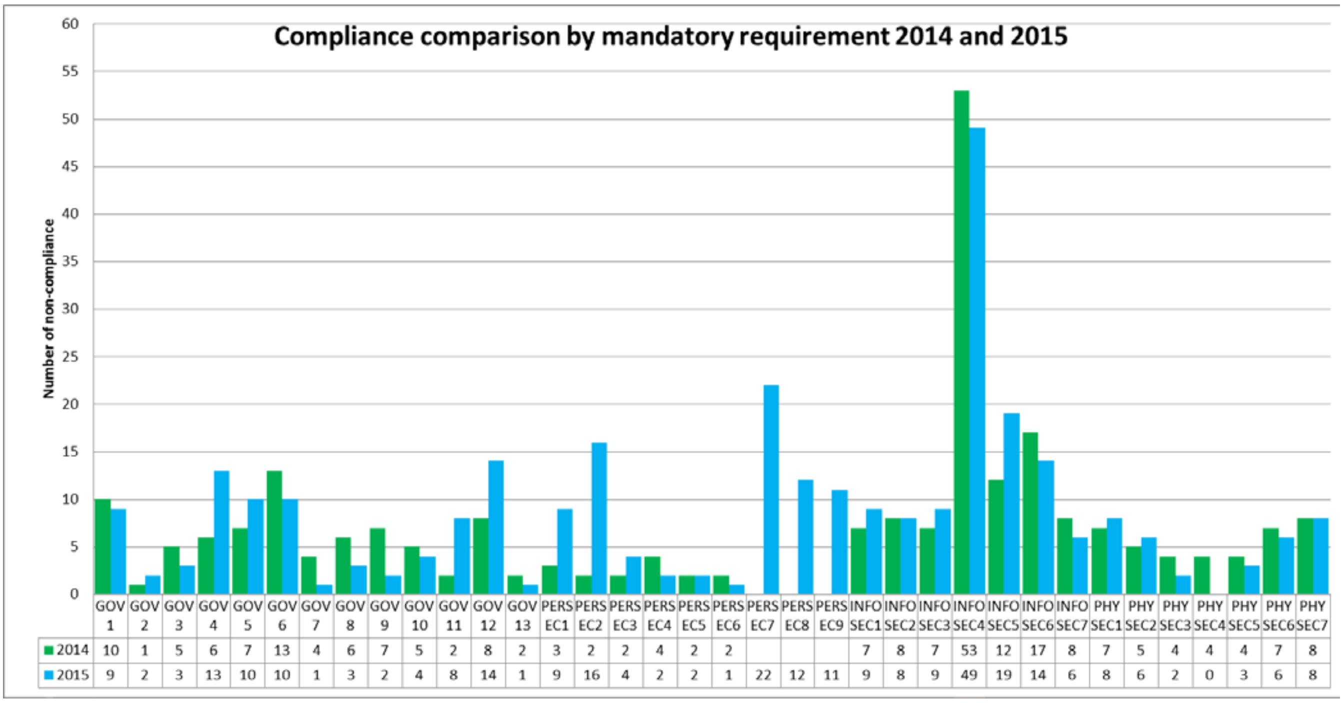
Information security is an important element of an agency's effective protective security regime. In 2014-15, information security represents the highest level of non-compliance of any PSPF component. Agency reporting indicates that information security is an ongoing risk for the Australian Government and is a challenge for a large number of agencies who have been unable to fully implement ASD's 'Top 4 Controls'. Agencies' non-compliance with each of the mandatory requirements in 2013-14 and in 2014-15 (described in full at **Attachment A**) are represented in *Figure 3*.

Information security is a dynamic policy area, which requires agility and flexibility to meet challenges posed by continuous technological advancement. A total of 49 agencies (48 per cent) reported non-compliance with INFOSEC-4 in 2014-15. This represents no change from 48 per cent of agencies non-compliant with this requirement in 2013-14. Thirteen agencies (18 per cent of those who reported non-compliance) reported INFOSEC-4 as their only area of non-compliance against the PSPF. AGD will work with ASD to assess whether additional support should be provided to agencies to assist with the implementation of the 'Top 4 Strategies' or if alternative mitigation strategies could be considered where INFOSEC-4 is not compatible with agency business.

INFOSEC-4 - Agencies must document and implement operational procedures and measures to ensure information, ICT systems and network tasks are managed securely and consistently, in accordance with the level of required security. This includes implementing the mandatory 'Strategies to Mitigate Targeted Cyber Intrusions' as detailed in the Australian Government Information Security Manual.

ASD advises that implementation of the 'Top 4 Strategies' represents a significant mitigation of 85 per cent of risk posed by targeted cyber intrusions. Achieving or maintaining higher levels of compliance against this requirement should be a priority for agencies in the next reporting period, to the extent practicable, taking into account business requirements.

example, 10 years for Negative Vetting 1) to the date the clearance was originally granted. Note that cases in progress are still captured as being overdue. This is consistent with ANAO methodology.



	GOV 1	GOV 2	GOV 3	GOV 4	GOV 5	GOV 6	GOV 7	GOV 8	GOV 9	GOV 10	GOV 11	GOV 12	GOV 13	PERS EC1	PERS EC2	PERS EC3	PERS EC4	PERS EC5	PERS EC6	PERS EC7	PERS EC8	PERS EC9	INFO SEC1	INFO SEC2	INFO SEC3	INFO SEC4	INFO SEC5	INFO SEC6	INFO SEC7	PHY SEC1	PHY SEC2	PHY SEC3	PHY SEC4	PHY SEC5	PHY SEC6	PHY SEC7
🟩 2014	10	1	5	6	7	13	4	6	7	5	2	8	2	3	2	2	4	2	2				7	8	7	53	12	17	8	7	5	4	4	4	7	8
🟦 2015	9	2	3	13	10	10	1	3	2	4	8	14	1	9	16	4	2	2	1	22	12	11	9	8	9	49	19	14	6	8	6	2	0	3	6	8

Figure 3: Agency non-compliance with each of the 36 mandatory requirements.

<u>Physical security (PHYSEC)</u>

Physical security elements of the PSPF are a combination of physical and procedural measures that agencies adopt to mitigate the risk of compromise by physical means of its people, information and assets. The 2014-15 compliance data suggests that agencies generally have a good understanding of the physical security requirements and their implementation. In 2014-15, physical security has the lowest level of non-compliance of any PSPF component. This may be due to physical security requirements tending to be more detailed, providing agencies with a greater level of clarity than other components, which rely more heavily on individual assessment of the threat environment and the risk appetite of each agency.

Next Steps

Culture of security

A fundamental aspect of successfully implementing and maintaining compliance with the PSPF is fostering a strong culture of security within an organisation. A strong and effective culture of security is critical to the success of all other security measures. An improved culture of security is achieved when Australian Government employees understand, accept and act upon their security responsibilities, integrate security into business practices, and adopt a proportional approach to identifying and managing potential threats and risks to security. A strong culture of security has clear intersections with integrity, performance and accountability. AGD is undertaking a body of work to support agencies to develop a strong culture of security.

Belcher Review

The efficiency and effectiveness of the PSPF was considered as part of the APS-wide *Independent Review of Whole-of-Government Internal Regulation* (Belcher Red Tape Review). The Belcher Red Tape Review made a number of recommendations, which the Secretaries Board has committed to implement. These include:

- Personnel security – to develop options to reduce the administrative burden of security vetting and improve security outcomes. The key recommendation involved applying a basic standard of employment screening for ongoing employees to replace Baseline security clearances. The report also recommended developing options to use electronic information sources for vetting, and developing a continuous assessment and evaluation model of security screening to reduce the administrative burden of the current processes.

- Governance – to review existing requirements to streamline the PSPF, improve AGD's communication and support to entities to implement the PSPF, and better integrate PSPF requirements with fraud requirements and anti-corruption measures.
- Information security – to incorporate the ISM produced by ASD into the PSPF. The review also recommended that Defence provide agencies with greater visibility of information about security clearances to enable those risks to be proactively managed in organisations.

Taking into account the significant risks associated with non-compliance with information security requirements, AGD will engage with ASD regarding alternative approaches or additional implementation support, with particular focus on INFOSEC-4.

AGD is separately considering possible changes to the way PSPF reporting will be conducted in the future to enable a streamlined and more nuanced reporting method to reflect the extent of implementation of the mandatory requirements of the PSPF.

Government Policy Order

Currently, the PSPF only applies to non-corporate Commonwealth entities. AGD is developing a government policy order (GPO) under the PGPA Act to extend the mandatory requirements of the PSPF to 85 CCEs and wholly-owned Commonwealth companies. AGD is undertaking an extensive consultation process with relevant entities and companies in accordance with PGPA Act requirements. The draft GPO aims to enable the consistent application of protective security policy across the Australian Government. The GPO extends the key requirements of the PSPF and sets out minimum protective security standards for the protection of Commonwealth resources held by the entity or company. AGD will ensure CCEs and Commonwealth companies have a sufficient period to commence implementation of the GPO's requirements, including reporting.

Attachment A: PSPF Mandatory Requirements

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

	- the heads of any agencies whose people, information or assets may be affected by the non-compliance.
GOV-8	Agencies must ensure investigators are appropriately trained and have procedures in place for reporting and investigating security incidents and taking corrective action, in accordance with the provisions of the: - *Australian Government protective security governance guidelines—Reporting incidents and conducting security investigations,* and/or - *Australian Government Investigations Standards*.
GOV- 9	Agencies 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	Agencies must adhere to any provisions concerning the security of people, information and assets contained in multilateral or bilateral agreements and arrangements to which Australia is a party.
GOV-11	Agencies must establish a business continuity management (BCM) program to provide for the continued availability of critical services and assets, and other services and assets when warranted by a threat and risk assessment.
GOV-12	Agencies must ensure the contracted service provider complies with the requirements of this policy and any protective security protocols.
GOV-13	Agencies must comply with section 10 of the *Public Governance, Performance and Accountability Rule 2014* and the *Commonwealth Fraud Control Policy.*
Personnel Security	
PERSEC-1	Agencies must ensure that their personnel who access Australian Government resources (people, information and assets): - are eligible to have access - have had their identity established - are suitable to have access, and - agree to comply with the Government's policies, standards, protocols and guidelines that safeguard that agency's resources from harm.
PERSEC-2	Agencies must have policies and procedures to assess and manage the ongoing suitability for employment of their personnel.
PERSEC-3	Agencies must identify, record and review positions that require a security clearance and the level of clearance required.
PERSEC-4	Agencies must ensure their personnel with ongoing access to Australian Government security classified resources hold a security clearance at the appropriate level, sponsored by an Australian Government agency.
PERSEC-5	Before issuing an eligibility waiver (citizenship or checkable background) and prior to requesting an Australian Government security clearance an agency must:

	• justify an exceptional business requirement • conduct and document a risk assessment • define the period covered by the waiver (which cannot be open-ended) • gain agreement from the clearance applicant to meet the conditions of the waiver • consult with the vetting agency
PERSEC-6	Agencies, other than authorised vetting agencies, must use the Australian Government Security Vetting Agency (AGSVA) to conduct initial vetting and reviews.
PERSEC-7	Agencies must establish, implement and maintain security clearance policies and procedures for clearance maintenance in their agencies.
PERSEC-8	Agencies and vetting agencies must share information that may impact on an individual's ongoing suitability to hold an Australian Government security clearance.
PERSEC-9	Agencies must have separation policies and procedures for departing clearance holders, which includes a requirement to: • inform vetting agencies when a clearance holder leaves agency employment or contract engagement • advise vetting agencies of any security concerns
Information Security	
INFOSEC-1	Agency heads must provide clear direction on information security through the development and implementation of an agency information security policy, and address agency information security requirements as part of the agency security plan.
INFOSEC-2	Each agency must establish a framework to provide direction and coordinated management of information security. Frameworks must be appropriate to the level of security risks to the agency's information environment.
INFOSEC-3	Agencies must implement policies and procedures for the security classification and protective control of information assets (in electronic and paper-based formats), which match their value, importance and sensitivity.
INFOSEC-4	Agencies must document and implement operational procedures and measures to ensure information, ICT systems and network tasks are managed securely and consistently, in accordance with the level of required security. This includes implementing the mandatory 'Strategies to Mitigate Targeted Cyber Intrusions' as detailed in the Australian Government Information Security Manual.
INFOSEC-5	Agencies must have in place control measures based on business owner requirements and assessed/accepted risks for controlling access to all information, ICT systems, networks (including remote access), infrastructures and applications. Agency access control rules must be consistent with agency business requirements and information classification as well as legal obligations.
INFOSEC-6	Agencies must have in place security measures during all stages of ICT system development, as well as when new ICT systems are implemented into the operational environment. Such measures must match the assessed security risk of the information holdings contained within, or passing across, ICT networks infrastructures and applications.

INFOSEC-7	Agencies must ensure that agency information security measures for all information processes, ICT systems and infrastructure adhere to any legislative or regulatory obligations under which the agency operates.
Physical Security	
PHYSEC-1	Agency heads must provide clear direction on physical security through the development and implementation of an agency physical security policy, and address agency physical security requirements as part of the agency security plan.
PHYSEC-2	Agencies must have in place policies and procedures to: • identify, protect and support employees under threat of violence, based on a threat and risk assessment of specific situations. In certain cases, agencies may have to extend protection and support to family members and others • report incidents to management, human resources, security and law enforcement authorities, as appropriate • provide information, training and counselling to employees, and • maintain thorough records and statements on reported incidents.
PHYSEC-3	Agencies must ensure they fully integrate protective security early in the process of planning, selecting, designing and modifying their facilities.
PHYSEC-4	Agencies must ensure that any proposed physical security measure or activity does not breach relevant employer occupational health and safety obligations.
PHYSEC-5	Agencies must show a duty of care for the physical safety of those members of the public interacting directly with the Australian Government. Where an agency's function involves providing services, the agency must ensure that clients can transact with the Australian Government with confidence about their physical wellbeing.
PHYSEC-6	Agencies must implement a level of physical security measures that minimises or removes the risk of information and ICT equipment being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.
PHYSEC-7	Agencies must develop plans and procedures to move up to heightened security levels in case of emergency and increased threat. The Australian Government may direct its agencies to implement heightened security levels.