Agency Security Plan

September 2020

Contents

Key information

Owner	Andre Remmers, Chief Security Officer (Branch Manager, Protective and Cyber Security)
Business unit	Protective and Cyber Security Branch
Filename	NDIA Agency Security Plan v5 Last saved 4/08/2021 8:25 AM
Contact for enquiries	Paul Trumble, Assistant Director, Security Policy Email: paul.trumble@ndis.gov.au Telephone: +61 2 6143 6022

Document version history

Version	Date	Comments
5.0	01/09/20	First version for SES consideration.

1. Foreword

The National Disability Insurance Agency (NDIA or the Agency) is committed to the effective management of its protective security risks across all tenancies and employees. We have in place protective security measures which assist in maintaining the capacity to operate and, as far as possible, ensure the safety and security of all personnel engaged in carrying out functions on behalf of the Agency, and the protection of our information and assets.

The Chief Executive Officer (CEO), with assistance from the Chief Security Officer (CSO) and Executive members, will continue to support a positive security culture throughout the Agency. This will promote a secure, efficient and effective method of delivering our business that allows employees, contractors, partners and visitors to work together securely in an environment of trust and confidence.

2. Introduction

The NDIA is the corporate Commonwealth entity responsible for implementing the National Disability Insurance Scheme (NDIS or Scheme). We are responsible for delivering the Scheme in a way that allows participants to exercise choice and control, and improves participant experience and outcomes. We must do this while safeguarding the long-term financial sustainability of the Scheme.

The Protective Security Policy Framework (PSPF) represents better practice for corporate Commonwealth entities. As a corporate Commonwealth entity, the Agency is required to adhere to the PSPF. The PSPF provides the appropriate controls for the Government and its agencies to protect people, information and property. One of these controls is the development of an Agency Security Plan (ASP or Plan) that meets the requirements of the PSPF.

In addition to the protection of these assets, the effective application of the PSPF also contributes to upholding the reputation of the Agency and the Government. This is imperative to ensure the Agency's roles as effective operator, trusted adviser and effective partner are maintained.

The Agency will maintain a strong security culture, and support risk treatments and controls that mitigate risk whilst enabling business outcomes. The Plan provides assurance that the Agency is effectively managing security risk and applying mandatory security governance arrangements to comply with the PSPF.

The Plan is part of the Agency's suite of protective security policy framework documents as outlined in the Agency's Security governance framework at Attachment A.

2.1 Scope

This plan applies to all employees, contractors, consultants, temporary workers and other workers in the Agency. They will be described as Agency personnel throughout this document.

2.2 Objectives

The Plan, as the overarching security document for the Agency, serves a range of functions and is intended to link the Agency's Corporate Plan with its obligations to effectively implement the PSPF and Information Security Manual.

The first objective outlines the security planning and compliance for the Agency, particularly in relation to the application and contextualisation of the PSPF.

The second objective articulates the Agency's security governance, and the application and integration of effective risk management into all decision making relevant to security.

3. Assessment of existing security measures

The NDIS began on 1 July 2013 for a three year trial period. In July 2016 the Agency began rolling out across Australia. Security has been an ever present concern, though it has been addressed in a sporadic manner with different business areas implementing their own security framework and solutions.

In late 2019 the Agency appointed its first Chief Security Officer (CSO). This was an important step to develop and implement a consistent and effective whole-of-agency security framework. This is the first version of the Plan. It enables the agency to consider its responsibilities under the PSPF and deliver compliant security measures.

The Agency has not performed an assessment of the existing security measures. The CSO's impression is that the basic security controls exist, however they are sporadic and are not supported by a security culture. Implementation of the ASP and supporting polices will enable the agency to address these issues.

The Agency's first security assessment is planned for Q3 2020. This will be performed in collaboration with Internal Audit to develop a security baseline. The completed assessment will be submitted to the Attorney General's Department and Minister. The findings of this audit will guide the CSO's work program for 2020-21 to develop and implement effective security controls.

The Agency's approach to monitoring, maturity assessment and reporting are addressed in the Plan.

4. Roles and responsibilities

The CEO, in conjunction with the CSO, is required to provide assurances to the Board as the Accountable Authority, that there are appropriate procedures for identifying resources at risk, and overseeing effective controls to mitigate security risks.

Whilst the CEO and CSO have final responsibility for all issues relating to protective security within the Agency, all agency personnel have a role in creating a positive security culture. These roles and functions are varied and are outlined in the below chapters.

In accordance with PSPF requirements, this Plan also articulates the security requirements of the CSO within an Accountable Authority.

4.1 All agency personnel

All Agency personnel are responsible for applying the security practices contained in the Agency's procedures, plans and policies. All agency personnel are ultimately accountable for their security behaviour, and must consider the impact of their conduct upon the Agency, and the reputation of the Commonwealth.

The Agency will ensure agency personnel are suitable to access Australian Government resources, and meet an appropriate standard of integrity and honesty as per the PSPF core and supporting requirements. Further information on this can be found in the Protective and Personnel Security Policies.

4.2 Agency people managers

People managers within the Agency are responsible for:

- ensuring staff and managers have the appropriate Australian Government security clearance to perform the functions of their role, both prior to, and while the employee is filling the position;
- understanding protective security requirements and providing guidance and leadership to their personnel about security attitudes and behaviours;
- ensuring that official information is correctly classified and is handled with care and in accordance with agency policy while in their business area (see the Protective Security Policy for further information);
- ensuring that staff and managers adhere to national and local policy and practices in relation to security threats or emergencies (see Agency Protective Security Incident Management Procedure);
- ensuring that staff undertake relevant security training, and as a minimum complete all mandatory security awareness programs required by the Agency; and
- reporting any issues and incidents of potential security significance to Protective and Cyber Security Branch.

4.3 Deputy Chief Information Security Officer

The Information Security Manual requires the Agency to have a Chief Information Security Officer (CISO). In the Agency, the Chief Information Officer includes the role of the CISO. The CISO provides strategic-level guidance for the Agency's cyber security program and ensuring compliance with cyber security policy, standards, regulations and legislation.

The Deputy Chief Information Security Officer (DCISO) oversees the day-to-day ICT security operations for the Agency, enacting and supporting the directives of the CEO, CSO and the CIO through the Agency Security Plan and Agency Cyber Security Strategy. They assist the CSO to monitor and manage ICT security systems and enterprise ICT security risks. The DCISO provides strategic ICT security advice in response to the agency cyber security threat environment. Their responsibilities include:

- ensuring new and established ICT systems have appropriate security controls implemented;
- monitoring information security for systems and respond to any cyber security incidents;
- monitoring the cyber threat and identify and advise system owners of appropriate security measures to meet the evolving threat landscape;
- providing executive reports on cyber security posture and associated risks for health systems and information;

- helping system owners to understand and respond to reported ICT audit failures;
- driving initiatives to foster a positive security culture throughout the Agency;
- delivering information Security awareness and training programs to personnel; and
- determining when an ICT security incident is serious or significant enough to commence an investigation.

4.4 Agency Security Adviser

The Agency Security Adviser (ASA) is responsible for strategic planning and ongoing management of the protective security environment within the Agency. The ASA is responsible for the coordination of physical, personnel and information security, and ensures the Agency's maturity against core requirements of the PSPF, whilst managing and reporting on security incidents and threats to the Agency's protective security. The ASA will develop security policy and protocols, and coordinate staff awareness programs. The ASA reports to the CSO and is supported by the Assistant Agency Security Adviser.

Whilst the roles of the DCISO and ASA are no longer mandated agency positions with specified learning requirements, the Agency has chosen to continue these as important Agency roles in managing our security arrangements on a day-to-day basis.

These occupants of these roles have or will be able to demonstrate competencies in, for example:

- a comprehensive knowledge of the PSPF and supporting technical guidance (e.g. ASIO Tech notes or the Australian Government ISM);
- technical competencies in security and the application of measures relevant to adviser functions (e.g. professional ICT certifications); and
- the management of security risk assessments.

4.5 Partners

Delivery of the NDIS is dependent on our relationship and work with a wide variety of government and non-government organisations. These organisations will be referred to as partners for the purpose of this Plan.

Many partners routinely accommodate Agency personnel to deliver the NDIS. The Agency retains responsibility for the security of its personnel, regardless of where they work and responsibility for its information and other assets where they are used by partners.

The Protective & Cyber Security and Partner Performance branches will implement security arrangements for the Agency in other organisations. This includes guidance to the Agency's expectations for security, as described in the Agency Security Plan, and associated policies and work health and safety for Agency personnel, information and assets.

5. Security management structures

To ensure the Agency makes security decisions in accordance with formalised security practices, a robust management structure needs to be in place. When implementing effective management structures and responsibilities; it is a requirement that those individuals within the structure be appropriately skilled, empowered and resourced. This is essential to achieving security outcomes for the Agency.

The core requirement for management structures and responsibilities is that the Agency must:

- appoint a CSO at the Senior Executive Service level to be responsible for security in the entity.
- empower the CSO to make decisions about:
    - the entity's protective security planning,
    - the entity's protective security practices and procedures, and
    - appointing security advisers within the entity; and
        - investigating, responding to, and reporting on security incidents, and
        - ensuring Agency personnel are aware of their collective responsibility to foster a positive security culture and are provided sufficient information and training to support this.

The following diagram represents the security governance structure.

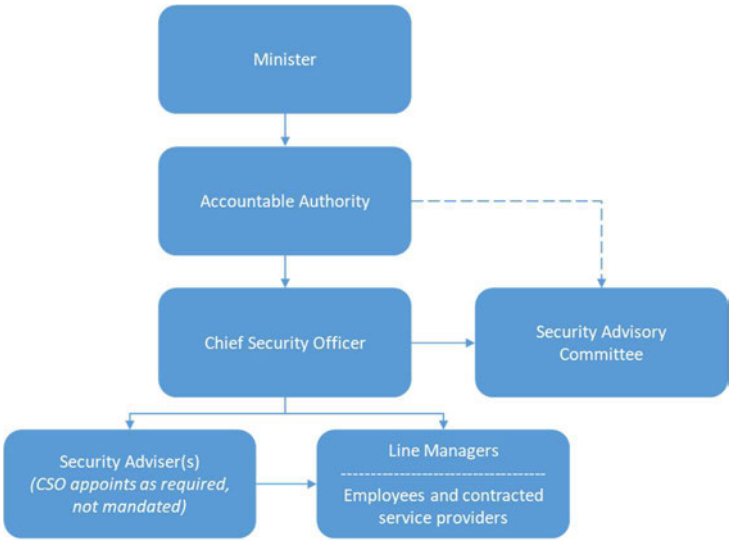

FIGURE 1 - NDIA OPERATIONAL SECURITY STRUCTURE

5.1 Chief Security Officer

The role of CSO had been delegated by the CEO to the Branch Manager Protective and Cyber Security, Mr Andre Remmers. Protective and Cyber Security Branch is responsible for the maintenance and record keeping in relation to this delegation.

The CSO defines the strategic direction and resources to deliver strategy, strengthen operations and improve the Agency's security culture and maturity. Effective security planning will ensure efficient and effective security practices across the agency. In conjunction with the Security Advisory Committee (SAC), the CSO will ensure agency security risks are managed and are flexible enough to adapt to change, minimise damage and disruption and build resilience.

The Agency Security Plan provides specific guidance against many of these aspects. It is the responsibility of the Protective and Cyber Security Branch to ensure that the Plan is current, and revised regularly.

The CSO is empowered to appoint security advisers. In making these decisions the CSO will:

- consider the scope and responsibilities delegated to each position within the context of the agency's risk environment, complexity of business, infrastructure, size and other relevant aspects;
- establish appropriate arrangements for managing the responsibilities of advisers. Where this results in security advisers not reporting directly to the CSO, the CSO maintains visibility of performance and outcomes;
- appoint advisers at a level that requires only broad direction in terms of delivering objectives, mission or functions;
- ensure the impact of security controls and treatments within the Agency are considered in terms of potential impacts on stakeholder and peer agencies;
- ensure delegations are sufficient to allow security advisers to undertake specific action in line with the policy of the entity, or to review previous actions or decisions in the work area; and
- determine the appropriate competencies, experience and specialist skills or qualifications required to undertake the appointed security role(s), including comprehensive knowledge of the PSPF/ISM.

The CSO will maintain a collaborative approach between appointed security advisers to ensure governance, information, personnel and physical security measures are complementary, promote robust security practices and achieve the agency's security objectives. CSO delegations relating to security advisers are maintained by the ASA.

Protective security practices reflect the Agency's implementation of the PSPF core (and supporting) governance, information, personnel and physical security requirements. The CSO, with advice from security advisers and SAC, is responsible for approving all relevant policy and protocols which will assist the Agency achieve its protective security goals.

If the Agency is unable to comply with part of the PSPF, the CSO will implement an alternative mitigation measure or control. The CSO will document the decision and adjust the maturity level for the related PSPF requirement.

The CSO is also responsible for authorising security investigations within the Agency. This policy, and the process of seeking approval, is addressed in the Protective Security Policy.

5.2 Protective and Cyber Security Branch

The Protective and Cyber Security Branch is responsible for much of the day-to-day planning and delivery associated with this Plan. The successful delivery of this Plan remains contingent on resourcing in terms of expenditure, staffing allocation and the security environment. The Branch's responsibilities include:

- managing the Agency's Security Risk Management Plan to ensure risks are appropriately managed.
- developing and maintaining protective security policies and procedures, including personnel, physical and information security.
- ensuring compliance with the Protective Security Policy Framework.
- managing security incident response arrangements.
- building security awareness through training and education.
- providing protective security advice to the Agency.
- managing building access arrangements and staff identification requirements.
- building a positive security culture in the Agency.

Protective and Cyber Security Branch has specialist advisors for; Agency, Regional, Information Technology, Personnel and Physical Security.

5.3 Security Advisory Committee

The Security Advisory Committee (SAC) monitors the Agency's preparedness to counter security threats and to report and makes recommendations to the Board as the Accountable Authority on any significant security risk management issues requiring its attention. The Committee will also establish well-designed security risk management policies, for ensuring (through the Chair) an appropriate level of senior management involvement and clarification of roles and responsibilities and appropriate training for staff with security responsibilities. The Committee will put into place systematic and coordinated security risk management processes, in order to identify, assess, treat and control protective security risks.

The SAC is chaired by the CSO and includes seven senior executives from:

- Participants and Planning Experience
- Participant Focus
- ICT Services
- Communications & Stakeholder Engagement
- People & Culture
- Strategy Development & Risk

- Corporate Services & CFO.

The most senior officer from each of the areas listed above shall appoint a representative to sit on the Committee. Members in the event of an emergency and with the prior agreement of the Chair may deputise others to attend on their behalf. Acting members should be of equal standing of the member they are replacing.

The SAC will report quarterly to the Board on its operation and activities during the previous three months.

6. Governance arrangements

The *Public Governance Performance and Accountability Act 2013*, requires that the agency governs in a manner which is consistent with Australian Government policies (including the PSPF). Governance arrangements in place within the Agency ensures that it manages known security risks and supports a positive security culture.

6.1 Security goals and objectives

The Agency security goals are to:

- implement protective security into all agency operations,
- establish a baseline of security maturity,
- develop a pathway to greater security maturity, and
- build a positive security culture.

The Agency security objectives are to maintain an environment that:

- safeguards participants, personnel and partners from foreseeable risks,
- facilitates the appropriate and authorised sharing of official information to deliver the Scheme,
- limits the potential for the compromise of the confidentiality, integrity and availability of its official information and assets,
- protects official assets from loss or misuse, and
- supports the continued delivery of the Scheme despite disruptions caused by all types of hazards.

6.2 Security risk management

Security risk management principles must be considered as part of critical decision-making processes within the Agency. The Board has approved our Risk Appetite Statement, which sets our appetite as conservative. The Board has set our appetite for risk as conservative. In practice, this means we must closely monitor and regularly review how we are managing the risks we face.

The CSO has applied this interpretation and tolerance to security risks. Accordingly, security risks will be monitored and reviewed so that our operations are properly designed and conducted to ensure there is no undue risk to the Agency, its assets, information or people.

The Agency's Risk Management Framework contextualises risk in terms of the Corporate Plan, ensuring clear links between risk and the Agency's goals. The Security Risk Management Plan uses the framework provided at the enterprise level to establish security specific threat assessments, risks, controls and treatments. This framework is maintained by the Protective and Cyber Security Branch, and is subject to annual review. The Agency Security Risk Register is part of this framework, however, this requires more regular updates. The Security Risk Register is tabled, discussed and considered at each meeting of the SAC.

The CSO, in conjunction with the Protective and Cyber Security Branch, is responsible for the application and maintenance of effective security risk management within the Agency.

6.3 Threat levels

The CSO is responsible for determining the Agency's threat level and implementing scalable controls to respond to threats. The CSO will consider:

- National Terrorism Threat Level Advisory System advice;
- protective security risk reviews;
- police advice;
- emergency management advice;
- Bureau of Meteorology advice;
- Agency security incident reports; and
- media reports.

The CSO will oversee the Agency's response to changing threat levels, working with the Emergency Response and Recovery Committee, Risk Committee, Security Advisory Committee and other business areas as appropriate. The CSO will take a risk based approach to the threat which may include:

- evaluating the business impact level;
- determining who needs to know about changes in the security threat level;
- outlining specific roles or responsibilities including who is responsible for determining the security alert level;
- ensuring personnel are aware of the measures employed by the entity to adapt to and mitigate emergencies and heightened threat levels; and
- detailing arrangements to monitor the threat level and review the security alert level when the entity undertakes significant new projects, the risk environment changes, or after a significant incident impacting the entity's ability to operate.

6.4 Business impact levels

It is mandated within the PSPF that the Agency must identify people, information (including ICT) and assets that are critical to the ongoing operation of the Agency and/or the national interest. Once these critical assets are identified then it must ensure that appropriate protections for these assets are in place to support the ongoing operations of its core government business. The Agency, as the subject expert for its core business, is best placed to:

- identify the people, information and assets which need safeguarding;
- determine the specific risks to our people, information and assets (risk assessment);
- identify the criticality of the Agency's people, information and assets (business continuity framework);
- identify the threats to the Agency's people, information and assets (threat assessments);
- assess the agency's degree of susceptibility and resilience to critical events (vulnerability assessment);
- assess the likelihood and impact of an identified event (risk analysis);
- implement protective security measures to mitigate or reduce the identified risks to an acceptable level (treat the risks);
- manage the untreatable residual risks and vulnerabilities; and
- identify an owner for each of the identified risks and have them accept responsibility for the risk.

The Agency has identified and considered risks and impacts against broad ranging information holdings and business processes. These are articulated in the Business Impact Levels Assessment. The maintenance and review of this document is the responsibility of the Protective and Cyber Security Branch.

6.5 Security reporting

The Agency is required to comply with the standards set out in the PSPF. In order to meet the requirements stipulated in the PSPF, the Agency must provide an annual report to its portfolio Minister, the Attorney-General's Department, the Auditor-General, and, where relevant, any other affected entities on:

- whether the entity achieved security outcomes and implemented requirements under the PSPF;
- the maturity of the entity's security capability;
- key risks to the entity's people, information and assets; and
- details of measures taken to mitigate or otherwise manage identified security risks.

The Agency must also report on its maturity level that could affect other entities whose interests or security arrangements could be affected by the outcome of unmitigated security risks, security incidents or vulnerabilities in our PSPF implementation.

The Agency will accomplish its reporting requirements by completing the PSPF Maturity Self-Assessment Report. The four level maturity model will allow the agency to determine real time implementation of the PSPF core requirements, better engage with risk by setting defendable risk tolerances and develop a road map for improvement into the future.

The four level maturity model allows the agency to identify how it achieves its standards, or maturity levels, regarding risk, culture, capability and performance relating to security. The maturity level descriptors are:

- **Ad Hoc** — Entity implementation of the PSPF core and supporting requirements is inconsistent and ad hoc. This provides limited protection of the entity's people, information and assets, potentially exposing the government to unmitigated security risks.
- **Developing** — The entity has implemented the majority of PSPF core requirements and has established a pathway for those requirements yet to be implemented. This provides partial protection of the entity's people, information and assets, potentially exposing the government to security risks.
- **Managing** — All PSPF core and supporting requirements are implemented and managed. This provides the minimum required protection of the entity's people, information and assets, consistent with policy requirements.
- **Embedded** – All PSPF core and supporting requirements are fully integrated into the entity's business. Security is proactively managed in response to the risk environment and better practice guidance informs entity's business and security decisions. This provides comprehensive protection of the entity's people, information and assets.

The above descriptors will provide an agency level, and objective, measurement of protective security policy implementation, and how it contributes to the PSPF principles, outcomes and core and supporting requirements which the Agency will report against.

Protective and Cyber Security Branch will develop and maintain a PSPF Remediation Plan after each annual report. Progress against this Plan and overall maturity will be reported to SGC who will ensure ongoing monitoring and management.

6.6 Security monitoring

Further to annual reporting requirements, the Agency will ensure the security environment is monitored regularly and effectively. This takes the form of quarterly 'dashboard' reports, prepared by the Protective and Cyber Security Branch within two weeks of a new calendar quarter having commenced. These dashboard reports are circulated to SAC and the Senior and Executive Leadership's Team and Audit and Risk Committee, and are required to provide updates on the following categories:

- Security Risk — this will include reference to all risks rated above the Agency risk tolerance
- PSPF Compliance and Maturity — current state assessment and projected levels for annual reports

- Personnel security data — including breakdown by clearance type, waivers and assessed positions
- Essential Eight compliance — including assessments of risk and maturity against each strategy
- Essential Eight updates — any information relevant to remedial or enhancement work conducted during the quarter
- Security infringements and incidents — de-identified information relating to incidents and infringements, including state-by-state breakdowns
- ICT alerts and monitoring — this will cover anomalous events, virus detection and other ICT security alerts
- Audit update — covering progress against any outstanding audit findings.

The Risk Committee is provided with a security briefing every three months regarding security arrangements in the Agency.

Ad hoc reports and briefings can also be requested through the CSO or Protective and Cyber Security Branch.

6.7 Incidents and security investigations

All security incidents will be centrally recorded by the Protective and Cyber Security Branch in Speak Up. This register is reviewed at each meeting of the SAC, with each incident considered for external review in accordance with guidance from the Attorney-General's Department. Staff guidance relating to security investigations can be found in the Agency Protective Security Policy.

Security Investigations will be conducted by appropriately authorised and trained personnel, strictly in accordance with the Agency Protective Security Policy as well as the Agency and APS Codes of Conduct. Protective and Cyber Security Branch will ensure relevant stakeholders are kept apprised of any investigations that might relate to Fraud or the Australian Public Service Values.

6.8 Contracted service providers

The Agency is bound to uphold the requirements of the PSPF and ISM in relation to all information and assets being accessed and managed by contractors and third parties.

Contract managers are ultimately responsible for ensuring contractors are provided with relevant information and tools to appropriately safeguard information and assets. Protective and Cyber Security Branch can provide assistance in reviewing and testing controls in place as part of a contractual arrangement.

Protective and Cyber Security Branch should also be consulted during the negotiation of any contracts that are likely to provide access or exposure to assets and information deemed to have a Moderate (or higher) Business Impact. Procurement managers can access the Business Impact Levels Assessment via the intranet.

6.9 Business continuity and disaster recovery

The Agency Business Continuity Framework is in place to describe a whole-of-business approach to ensure critical services can be returned to normality in a timely fashion. This function is currently managed by the Risk Branch.

Protective and Cyber Security Branch plays an important part in business continuity, particularly in its role on the Emergency Response and Recovery Committee. Protective and Cyber Security Branch will identify people, information and assets that are critical to the ongoing operation of the Agency, and apply appropriate protections to these resources.

The CSO will oversee the application of Agency and Commonwealth security policy during and after all Business Continuity events. Breaches of security during these events will be recorded by Protective and Cyber Security Branch on the Security Incident Register, and reported as part of any relevant reporting.

6.10 Fraud control

The NDIS Fraud Taskforce was established in July 2018, a partnership between Agency the Australian Federal Police and the Department of Human Services (now Services Australia). The Fraud Taskforce identifies and investigates potential serious and organised fraud against the NDIS and will strengthen longer-term fraud prevention and detection activity and capability within the Agency.

Protective and Cyber Security Branch must ensure all security incidents and investigations that may indicate the presence of fraudulent activity are referred to the Agency Fraud Control Officer.

6.11 Security audit

Security audits are an important part of quality assurance, and also serve to assist the Agency evaluate the effectiveness of controls.

Protective and Cyber Security Branch will cooperate with internal and external audits, with a view to providing timely and accurate information. The Agency may conduct internal audit reviews into any aspect of ISM or PSPF maturity and compliance. The Australian National Audit Office (ANAO), may conduct performance reviews on any aspect of the Agency's security arrangement and or compliance. This could be Agency specific or as part of a broader review. This is important in terms of the Commonwealth's approach to managing risk. The Protective and Cyber Security Branch is required to ensure CSO is aware and briefed of relevant ANAO commissioned security audits.

Where remedial work or recommendations are made as part of an audit report, SAC is authorised to oversee the implementation and evaluation of these. Progress against outstanding audit recommendations will also be included in Quarterly Dashboard Reports for the SAC.

6.12 Security Quality Assurance Framework

The Security Quality Assurance Framework (Attachment B) is a scheduled work program by which Protective and Cyber Security Branch provides assurance to the Agency that the security controls and methodologies in place are tested, evaluated and effective in meeting the Agency's security requirements.

The Security Quality Assurance Framework (SQAF) is reviewed monthly and offers Agency assurance across each of the 16 core requirements of the PSPF over the course of a year. Whilst the development of the SQAF should prioritise high-risk controls to ensure their effectiveness, of it is also important to balance these checks and balances with routine reviews. To this end the SQAF will ensure at least one of the checks conducted each month results in a LOW risk rating, as defined in the Agency Security Risk Management Framework.

The Agency Security Plan and all supporting policies will be reviewed at least every two years to determine the adequacy of existing measures and mitigation controls, and respond to and manage significant shifts in the risk, threat and operating environment.

7. Agency security measures

The information below outlines how the Agency will meet its obligations in complying with the mandatory requirements of the PSPF and the controls it must adhere to.

7.1 Personnel security

The Agency will ensure its personnel are suitable to access Australian Government resources, and meet an appropriate standard of honesty, integrity and tolerance throughout the period of their engagement. The Agency will achieve this goal by ensuring:

- robust and integrated onboarding, Pre-Engagement Checks, maintenance and separation procedures are in place; and
- the establishment of strong personnel security practices, underpinned by an effective and current Agency-wide security clearance and Designated Security Assessed Positions (DSAP) register.

The Agency Protective Security Policy articulates how the Agency has integrated and implemented these personnel security objectives, as well as the core requirements for personnel who hold a clearance and have access to sensitive or security classified assets.

The Agency Security Awareness and Training Plan is also an important part of Personnel Security. This Plan articulates the regularity and content of training programs, communications strategies and awareness strategies for staff. Content of the Security Awareness and Training Plan shall include induction and annual refresher training, ICT Security training, overseas travel briefs (where appropriate), contact reporting, clearance aftercare and maintenance and diverse awareness strategies designed to build the Agency's security culture.

Personnel Security controls are reviewed by Protective and Cyber Security Branch on a monthly basis, as defined in the Security Quality Assurance Framework (Attachment B).

7.2 Information security

The Agency has significant personal and sensitive information holdings with a large funding and distribution base. This exposes the Agency to numerous information and cyber security risks. We need to ensure that our systems and data are resilient to information security risks and cyber-attacks and remain secure, available and reliable. The Agency faces a lot of internal and external change drivers, as noted below:

- our security culture is unique and evolving – Security is not a primary function of the Agency. The majority of Agency's end users have varied levels of information and cyber security awareness;
- there is an increasing appetite for business driven technology initiatives involving emerging technologies and delivery models;
- our business areas and stakeholders are demanding access to Agency resources, information and services 24x7 across multiple devices from any location. The very innovations that drive business growth create cyber security risks and increase the need for real time threat intelligence and response; and
- stakeholders expectations of 'Data Protection and Stewardship' are increasing with a number of high profile cyber security incidents involving loss of personal and sensitive data.

The Agency has a clear plan to appropriately safeguard its information (and information systems) to ensure the confidentiality, integrity and availability of that information to those with a need-to-know. The following are the key principles/directions that underpin the Agency's information security arrangements:

- correctly identify the information and assets we hold, and appropriately classify and handle this information (as per the classification requirements of the PSPF) through its lifecycle.
- enable appropriate access to official information including the sharing of information, ensuring need-to-know
- mitigate targeted cyber intrusions and emerging cyber threats by managing risk, enhance cyber-resilience and achieving and maintaining compliance
- have security measures in place during all stages of ICT system development, including certifying and accreditation of ICT systems when implementing in the operational environment.

A detailed set of policies and procedures has been developed to provide additional detail and guidance on how the above-noted information security principles/directions will be operationalised. The Agency Cyber Security Strategy has been developed which sets out Agency's guiding principles, objectives and cyber security initiatives to lift the maturity of the Agency. The Agency Cyber Security Strategy and the information security related policies and procedures are available on the Intranet.

Information Security controls are reviewed by Protective and Cyber Security Branch on a monthly basis, as defined in the Security Quality Assurance Framework (Attachment B).

7.3 Physical security

The Agency must ensure it provides and maintains a safe and secure physical environment for its people, information and assets. The Agency will achieve this in three ways:

- Managing its physical resources to minimise or remove the risk of resources, including information and ICT resources, being made inoperable or accessed by those without authorisation. This includes the use and or removal of information without appropriate authorisation.
- When planning and modifying entity facilities, the Agency will fully integrate protective security early in the process of planning, selecting, designing and modifying its facilities.
- Monitoring security environments in and around Agency tenancies to ensure the quality and reliability of physical security controls remain effective and fit-for-purpose.

The Agency will also maintain a Site Security Plan (SSP) for each separate tenancy. These will specify what controls have been selected to secure the facility both from an administrative and technical perspective. The SSP will determine whether existing physical security measures appropriately demarcate security zones and restricted access areas, including an implementation and testing plan associated with electronic access control and alarm systems. A physical assessment must be completed every two years. The SSP is to be reviewed as soon as possible after a major security incident occurs at the facility, and be updated to reflect changes to business or identified new risks within the two-year period.

The future selection, design and modification of accommodation used by the Agency will ensure that physical access controls are maintained to satisfy the security zone requirements applicable at that time. Mandatory requirements regarding the certification of security zones and completion of SSP are outlined in the Physical Security Policy.

For staff working outside of Agency tenancies, guidance is available in the Agency's Home Based Work Policy and within the Protective Security Policy.

The Agency has an agreed approach regarding physical security controls in the event there is a change to the Agency's threat. This might arise as a result of a specific or targeted threat to the Agency or its people, or in conjunction with the National Terrorism Advisory System, commonly referred to as the National Alert Level. This approach is articulated in the Agency Increased Threat Procedure, managed by Protective and Cyber Security Branch.

Physical Security controls are reviewed by Protective and Cyber Security Branch on a monthly basis, as defined in the Security Quality Assurance Framework (Attachment B).

Attachment A: Security governance framework

Category	Policies
Overarching documents	• CEO Security Directive • Agency Security Plan • Protective Security Policy
Governance	• Risk Appetite Statement* • Risk Management Framework* • Business Continuity Management Policy* • Fraud Control Plan* • Security Quality Assurance Framework Policy • Procurement Policy*
Information	• ICT Security Policy • Systems authority to operate • Cloud services Policy
Personnel	• Personnel Security Policy • Access to Official Information and Resources Policy • Designated Security Assess Position Register Policy • Separation Policy • Managing Unreasonably Behaviour Policy
Physical	• Physical Security Policy • Physical Security Design Standards • Electronic Security Design Standards • Site Security Plan Policy • Site Security Plans

*not owned by the CSO

Attachment B: Security Quality Assurance Framework

Core Requirement	s47E(d) - certain operations of agencies
1. Role of accountable authority	
2. Management structures and responsibilities	
3. Security planning and risk management	
4. Security maturity monitoring	
5. Reporting on security	
6. Security governance for contracted goods and services providers	
7. Security governance for international sharing	
8. Sensitive and classified information	
9. Access to information	
10. Safeguarding information from cyber threats	
11. Robust ICT system	
12. Eligibility and suitability of personnel	
13. Ongoing assessment of personnel	
14. Separating personnel	
15. Physical security for entity resources	
16. Entity facilities	
Overall	

Attachment C: 2020-21 Plan

Quarter	Tasks
July 2020 to September 2020	• First Security Advisory Group meeting • CEO approves Agency Security Plan and CEO's Directive • Internal audit on security maturity (Agency security baseline) • Approval of all Security framework policies • Submission of security assessment • Begin PITC Engagement / Information Gathering • Start review of eligibility and suitability of personnel • Develop program of site security reviews for all facilities
October 2020 to December 2020	• Update Security Intranet pages • Security Advisory Group meeting • Begin engagement with Procurement Operations Team to incorporate security into the Procurement Policy • Begin engagement with Business Continuity to incorporate security into the Business Continuity Management Policy • Partner Pilot Support Project • Review all security assessed positions • Conduct site security reviews as per program
January 2021 to March 2021	• Security Advisory Group meeting • Conduct site security reviews as per program • Start Partner Security Framework pilot.
April 2021 to June 2021	• Security Advisory Group meeting • Conduct site security reviews as per program • Develop new 2021-22 Plan • Review Agency Security Plan

Approved: 02/11/2021

Owner: BM Protective & Cyber Security

Contact: security@ndis.gov.au

Security Quality Assurance Policy

1. Purpose

The NDIA CEO's Directive on Security established the importance of security and compliance with the Protective Security Policy Framework for the Agency.

The governance requirements of the PSPF define the expectation of the Agency to monitor and asses the maturity of its security capability and risk culture. This Policy describes how the Agency will perform its security quality assurance and how this is embedded into agency governance and assurance practices.

2. Definitions

CSO: Chief Security Officer – the Senior Executive who is responsible for the Agency's security and accountable to the CEO and Board. The CSO is the Branch Manager of Protective and Cyber Security Branch.
Maturity: A measure of the NDIA's capability in relation to security policy and culture.
PSPF: Protective Security Policy Framework – the government's protective security policy which has been implemented by the NDIA.
SAG: Security Advisory Group – a group chaired by the CSO to make decisions under delegation and provide advice and recommendations to the CEO, Board and ELT regarding agency security.
Security Capability: The security position in relation to core and supporting requirements of the PSPF.
Security risk culture: The NDIA's system of values and its personnel's behaviours, attitudes and understanding that are related to security risk that shapes the risk decisions of the entity leadership and personnel.

3. Objective

The objectives of this Policy are to define and establish a methodology for the NDIA to:

- assess security capability maturity
- assess security risk culture
- develop security maturity to a high level.

4. Policy application

The Agency Security Plan provides an overview of how the Agency will implement security policy and achieve compliance with the PSPF. Compliance with the PSPF is expressed in terms of maturity of compliance with the PSPF's core requirements.

4.1 Security capability maturity

Security capability maturity refers to the NDIA's security position in relation to its specific risk environment and risk tolerances. This includes acknowledging the successes and effectiveness of PSPF implementation, as well as highlighting areas for improvement.

The Agency uses the PSPF Maturity Self-Assessment Model. This has four maturity levels:

- **ad hoc**: partial or basic implementation and management of PSPF core and supporting requirements
- **developing**: substantial, but not fully effective implementation and management of PSPF core and supporting requirements
- **managing**: complete and effective implementation and management of PSPF core and supporting requirements
- **embedded**: comprehensive and effective implementation and proactive management of PSPF core and supporting requirements and excelling at implementation of better-practice guidance.

The PSPF considers managing to be the baseline maturity level. The NDIA aims to achieve maturity of at least managing for all security requirements.

4.2 Security risk culture

Security risk culture is the agency's system of values and its personnel's behaviours, attitudes and understanding that are related to security risk that shapes the risk decisions of the entity leadership and personnel. A mature risk culture is a fundamental enabler of good government business.

The NDIA's risk culture is driven by the CSO, with support and championing of risk culture by the CEO, Board and Executive Leadership Team.

Protective and Cyber Security Branch will take action to develop a mature risk culture through a Strategic Communication Plan, implementation of suitable security practices in different business activities and other actions as appropriate.

4.3 Security maturity

Monitoring security maturity is an ongoing process and involves routine assessment of the entity's security capability and risk culture against the core requirements of the PSPF.

Security maturity will be continuously monitored by Protective and Cyber Security Branch. The CSO, Agency Security Advisor and other personnel will monitor the agency's security capability and take a proactive approach to known issues.

At the end of every financial year, the Branch will conduct a detailed annual security report using the PSPF template. This will be submitted to the CSO who will present it to the Security Advisory Committee (SAC) and CEO.

At the end of every quarter, ahead of the SAC meeting, Protective and Cyber Security Branch will perform a basic maturity assessment to identify any issues for SAC consideration.

Where appropriate, the CSO will raise security maturity issues with the Risk Committee, other committees where appropriate or out of session with the SAC.

5. Procedure

This policy is supported by the current version of the Security Quality Assurance Procedure ('the Procedure') and the procedures referred to therein.

6. Key principles

The following key principles underpin the NDIA's approach to security quality assurance:

- The CSO is responsible for implementing security policy and security quality assurance.
- The Agency will constantly perform security quality assurance activities to proactively identify and address issues.
- A detailed analysis for security maturity will be carried out at the end of every financial year.
- The CSO and Security Advisory Group will oversee the agency's security maturity and drive action at the Executive level.
- The CSO and PCS will take a range of actions to develop the agency's security culture.
- Developing security maturity and culture to a high level is a priority for the agency. It is recognised that this is a long term change.

7. Mandatory Requirements

This Policy is part of the Agency's PSPF compliance. It is mandatory that the CSO and PCS follow the current Security Quality Assurance Policy and Procedure.

Other business areas must comply with any security maturity related requests for information, change, risk management etc.

All Agency personnel must contribute to a mature security culture.

8. Relevant legislation

This Policy is supported by Commonwealth legislation including:

- Public Governance, Performance and Accountability Act 2013
- National Disability Insurance Scheme Act 2013
- National Disability Insurance Scheme – Risk Management Rules 2013

Other

- Protective Security Policy Framework
- Information Security Manual

Approved: 20/11/2020

Owner: BM Protective & Cyber Security

Contact: security@ndis.gov.au

The content of this document is OFFICIAL.

Personnel Security Policy

1. Purpose

This Personnel Security Risk Assessment is part of broad ranging controls designed to protect the Agency's people, information, assets and reputation. In conjunction with the Agency Security Plan, Agency Protective Security Policy this risk assessment will allow the Agency to:

- Deliver a level of assurance about how the Agency conducts its pre-employment and onboarding procedures, therefore ensuring the credentials and integrity of the Agency's workforce;
- Identify the Agency's personnel security vulnerabilities, such as insider threats, and identify appropriate countermeasures through the Agency's pre-employment screening process to mitigate the risks;
- Communicate risks and risk solutions to senior management and secure their engagement in implementing controls and further treatments;
- Effectively allocate resources commensurate with the level of risk, to complement existing personnel security controls; and
- Continually monitor the effectiveness of mitigation controls.

This risk assessment has been conducted in accordance with guidance outlined in the Protective Security Policy Framework (PSPF), and relevant Standards Australia publications.

2. Definitions

Accountable Authority: The NDIA Board, who is responsible for our operations under Section 12 of the Public Governance, Performance & Accountability Act 2013.
AS: Australian Standards
APS: Australian Public Service
ASP: Agency Security Plan the NDIA's response to the PSPF which outlines the Agency's protective security arrangements
ICT: Information and Communication Technology
ISM: Information Security Manual
IT: Information Technology
NDIA: National Disability Insurance Agency (or the Agency)
NDIS: National Disability Insurance Scheme (or the Scheme)

Protective Security: The Government's path to protect people, information, assets and reputation
PSPF: The Protective Security Policy Framework
RAS: Risk Appetite Statement

3. Objective

This assessment supports the Agency Security Plan, Agency Enterprise Risk Management Plan and Agency's Employment terms and conditions. This document utilises identical risk definitions, and has been assessed in the context of broader risk within the agency. The Agency Business Impact Levels Assessment has also been referenced in terms of business and program risk – specifically in relation to personnel accessing systems and data.

The risks considered in this assessment are defined on three levels:

- **Agency risks** – risks that are Agency wide and directly affect Agency business;
- **Program risks** – risks that are directly associated with a program or package of work undertaken within the Agency; and
- **Individual risks** – risks that are derived from personnel working in the Agency.

Specific risks may relate to more than one of the above levels. Where this is the case it will be noted in the relevant definitions and risk table.

4. Policy application

Background

The NDIA is the corporate Commonwealth entity responsible for implementing the National Disability Insurance Scheme (NDIS). We are responsible for delivering the Scheme in a way that allows participants to exercise choice and control, and improves participant experience and outcomes. We must do this while safeguarding the long-term financial sustainability of the Scheme.

The Protective Security Policy Framework (PSPF) represents better practice for corporate Commonwealth entities. The Accountable Authority has decided that the Agency, as a corporate Commonwealth entity, will adhere to the PSPF. The PSPF provides the appropriate controls for the Government and its agencies to protect people, information and property. One of these controls is the development of an Agency Security Plan (ASP) that meets the requirements of the PSPF.

In addition to the protection of these assets, the effective application of the PSPF also contributes to upholding the reputation of the Agency and the Government. This is imperative to ensure the Agency's roles as effective operator, trusted adviser and effective partner are maintained.

The Agency will maintain a strong security culture, and support risk treatments and controls that mitigate risk whilst enabling business outcomes.

This risk assessment considers and contextualises the specific risks associated with personnel security, and the various measures that can be taken to mitigate them.

Personnel security

Personnel security is a system of policies and procedures that seek to manage the risk of people exploiting, or having the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes. This threat is commonly referred to as

'trusted insider' and is recognised as posing one of the most significant risks to an agency and/or the Government. [1]

Personnel Security is widely recognised as one of the four core categories of Protective Security (in conjunction with Physical, Information and Information Communication Technology (ICT) Security), and there are various controls and compliance requirements for all Commonwealth agencies outlined within the policy and protocols documents comprising the PSPF.

In addition to this risk assessment, the Agency addresses compliance, maturity and personnel security practices in a range of key governance documents. These are:

- Agency Security Plan;
- Agency Protective Security Policy; and
- Agency Risk Management Framework.

Personnel security controls include addressing risks across; recruitment (security vetting and clearances), onboarding, pre-employment screening, effective staff management (ongoing suitability), training and incident reporting.

The trusted insider

The PSPF defines the 'trusted insider' as potential, current or former employees or contractors who have (or have had) legitimate access to information, techniques, technology, assets or premises. These people are motivated by a range of factors, but are broadly described in two categories:

- **Unintentional Insider**: Unintentional Insiders are trusted employees or contractors who inadvertently expose, or make vulnerable to loss or exploitation, privileged information, techniques, technology, assets or premises. Inadvertent actions include poor security practices (such as leaving IT systems unattended and failure to secure sensitive documents), and unwitting unauthorised disclosure to a third party.
- **Malicious Insider**: Malicious Insiders are trusted employees and contractors who deliberately and wilfully breach their duty to maintain the security of privileged information, techniques, technology, assets or premises.

Malicious insiders can be categorised into two types:

- **Self-motivated insiders** are individuals whose actions are undertaken of their own volition, and not initiated as the result of any connection to, or directions by, a third party.
- **Recruited insiders** are individuals co-opted by a third party to specifically exploit their potential, current or former privileged access. This includes cultivated and recruited foreign intelligence, or their entities, with malicious intent.

Identified personnel security threats

Whilst the trusted insider is recognised as the primary threat-source to personnel security, there are other broad ranging threats which the Agency attempts to mitigate by utilising a robust employment screening process. The identified threats, as listed in the Agency Security Risk Management Plan are:

- Theft of assets and information;
- Misuse of assets and information;

[1] ANAOs Mitigating Insider Threats Through Personnel Security (ANAO Report No. 38 2017-18)

- Disclosure of information;
- Sabotage of assets and information systems;
- Compromise of information;
- Facilitating unauthorised access to assets;
- Direct attack on personnel or assets; and
- Inappropriate disposal of assets.

4.1 Agency Security Risk Environment

The Agency's Risk Management Framework and Policy define effective and appropriately documented risk management. These practices complement the maturity based compliance reporting of the PSPF.

The Agency is able to engage with security risk when operational or business requirements override basic compliance, but only when suitable controls and risk acceptance have been addressed.

Risk appetite

Risk appetite is the amount of risk an entity is willing to accept or retain in order to achieve its objectives.

Risk tolerance is a specific level of risk taking that is acceptable, or not acceptable, in order to achieve a specific objective or manage a category of risk. Risk tolerance represents the practical application of risk appetite and is most effective when it is understood by all Agency officials.

The Board has approved the Risk Appetite Statement (RAS). The RAS provides us with a consistent approach to how we manage our risks. The Board has set our appetite for risk as conservative which recognises the continued growth and the challenges we face with rolling out a ground-breaking Scheme.

This means that we must closely monitor and regularly review how we are managing the risks we face.

PSPF and ISM compliance

The PSPF and the Information Security Manual (ISM) are Commonwealth policy documents that outline minimum standards and controls in relation to Protective and IT security risk. Annual compliance reporting relating to both frameworks is required.

The Agency's compliance strategy is described in the Agency Security Plan. Personnel Security compliance with the PSPF and ISM is approved in the Protective Security Policy.

The Personnel Security Risk Assessment contextualises and articulates effective risk management principles and procedures for Personnel Security. This ensures Senior Management is able to make informed and transparent choices in relation to compliance or operational needs.

Information security

The Agency has a range of information systems, which are hosted by Services Australia. The Agency strives to ensure adequate technical, logical and administrative controls in place to protect the confidentiality, integrity and availability of the information it collects, processes and stores on behalf of its stakeholders. The technical controls are primarily delivered by Services Australia. The administrative and logical controls of these controls rely on effective implementation by Agency staff and contractors. This assessment considers the personnel security controls that are implemented to mitigate risks posed to information and systems by these personnel.

Information and systems

The Agency manages important information and information management systems on behalf of the Commonwealth. The Agency's Business Impact Levels Assessment notes that the compromise of some Agency systems and information meets the Commonwealth threshold for a HIGH business impact. Risks include those events that impact the confidentiality, integrity or availability of these systems and information.

The protection of these systems and information is paramount. However this must be balanced with the requirement for the information to be useable and accessible to those with a genuine need-to-know. Due to the need-to-share status of this information, some administrative and technical controls that would traditionally be employed to protect information assets have had to be replaced with additional checks and balances.

These additional checks and balances relate primarily to ensuring that those with significant or administrative access to this information are demonstrably fit and proper people. This can be demonstrated through pre-employment checking, as well as through the security clearance and maintenance process.

Commonwealth entity

As a Corporate Commonwealth Entity, the Agency has a responsibility to maintain the reputation, professionalism and effectiveness of the public sector and the government of the day. There are recent incidents of Commonwealth agencies not performing appropriate pre-employment or suitability checks, which have resulted in actual or perceived conflicts and damage.

Whilst the Agency is a low risk agency, our approach to personnel security must take into account the Commonwealth's policies and practices in relation to national security, incident reporting and threat assessments.

Compliance and Investigations

The Agency has a compliance and investigative role that necessitates establishing contact with a significant cross section of the Australian public. This could include motivated threat actors, such as criminals and members of organised criminal groups. It is in the administration of the NDIS system that staff have the potential to come into contact with people from these groups, which may expose them and our assets to harm.

Furthermore, these threat actors may seek influence through infiltration or compromise of Agency personnel. Appropriate checks and balances should be maintained to ensure that personnel accessing or amending official information and records are fit and proper, and there are no conflicts of interest.

4.2 Agency Employment Screening

Section 4.4 of the Agency Protective Security Policy provides an overview of the Agency's onboarding procedure. The agency's onboarding is underpinned by:

- Australian Standard 4811-2006 – Employment Screening (AS 4811); and
- PSPF core and supporting requirements for personnel security, namely the eligibility and suitability of personnel. A Risk Assessment into the Agency's employment screening process can be found below titled Entry Screening Assessment.

Employment screening requirements

The agency's employment screening requirements are, in part, guided by AS 4811. The screening requirements are applied to ongoing and non-ongoing APS staff, and contractors.

The requirements are based on mandatory checks, recommended checks under AS 4811 and additional checks specific to the Agency. See table below for a list of the Agency's employment screening requirements.

Employment Screening Checks
Mandatory requirement for employment screening
Identity Check: • One document from 'Commencement of Identity" category • One document from 'Primary Use in the Community' category • Two documents from 'Secondary Use in the Community' category
Recommended checks under Australian Standard 4811-2006: Employment Screening
• Five year residency check – Details requested in order to conduct the police check
• Five year employment check
• National Police check - commonly referred to as Police records check
• Professional referee check
• Personal character reference
• Qualification verification – Document Verification Service provided by Services Australia
Additional checks specified by the Agency
• Suitability questionnaire – This requirement is replicated in the various declarations that prospective employees and contractors must submit.
• Official Secrets Acknowledgement
• Deed of Confidentiality

Eligibility and suitability requirements

The agency must follow directions which are mandated within Australian Government Protective Security Policy Framework (PSPF). For onboarding, the PSPF core requirement document Eligibility and Suitability of Personnel outlines v2018.0:

- Pre-employment screening, to be undertaken to Australian Standards 4811, which is the primary activity used to mitigate the Agency's security risks; and
- The use of security clearances, to be conducted by the Australian Government Security Vetting Agency (AGSVA), where an additional level of assurance of the suitability and integrity of an employee is required. This could be for access to security classified information, or to provide greater assurance for designated security assessed positions.

5. Procedure

This Policy is implemented through the following Procedures:

- Agency Protective Security Policy
- Agency Security Plan
- Agency Risk Management Framework
- Agency Enterprise Risk Management Plan
- Agency Employment terms and conditions

6. Key principles

The following key principles underpin the NDIA's approach to risk management for Personnel Security:

- The NDIA is committed to delivering the NDIS in a way that allows participants to exercise choice and control, and improves participant experience and outcomes.
- The Protective Security Policy Framework (PSPF) represents better practice for corporate Commonwealth entities. The PSPF compliance strategy, described in the Agency Security Plan, Protective Security Policy, and will ensure NDIA adherence to the PSPF.
- Personnel security is a system of policies and procedures that seek to manage the risk of people exploiting, or having the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes.
- This risk assessment considers and contextualises the specific risks associated with personnel security, and the various measures that can be taken to mitigate them.

7. Mandatory Requirements

All personnel will follow the Personnel Security Risk Management. When a worker is to join the NDIA or move to another role, it is mandatory that:

- The Manager ensures the worker has passed the pre-engagement screening requirements,
- The worker has an appropriate security clearance for the work,
- Role and site specific personnel security risks are addressed as soon as possible.

8. Relevant legislation

This Policy is supported by Commonwealth legislation including:

- Australian Government Information and Communications Technology Security Manual (ISM) 2016
- Australian Government Protective Security Policy Framework (PSPF)

Other references

- ANAO Mitigating Insider Threats Through Personnel Security
- Australian Standard 4811-2006 – Employment Screening
- The Australian Government Security Vetting Agency (AGSVA) – Central Vetting Agency for the Australian Government and conducts security clearances assessments for federal, state and territory agencies
- Risk Management Standards (AS/NZS ISO 31000:2009)
- Work Health and Safety Act 2011