FSDF SPATIAL INFORMATION MANAGEMENT POLICIES – SECURITY

Objective: Securing the Foundation Spatial Data Framework.

This document is presented by ANZLIC – the Spatial Information Council, representing the Australian and New Zealand Governments, and the governments of the States and Territories of Australia.

The Australian and New Zealand Foundation Spatial Data Framework:
FSDF Spatial Information Management Policies - Security.

About this document

This document has been published by the Department of Communications on behalf of ANZLIC—the Spatial Information Council. ANZLIC is an intergovernmental council that comprises representatives from the Australian, state and territory governments and the New Zealand Government. The ANZLIC Secretariat is currently provided by the department.

Digital versions of this publication are also available on the ANZLIC website at www.anzlic.org.au/**FSDF**.

Copyright notice

Contact details

For information about ANZLIC—the Spatial Information Council or if you would like more information on this document, please contact:

ANZLIC Secretariat
Department of Communications
GPO Box 2154
Canberra ACT 2601
Phone: 02 6271 1493 (international +61 2 6271 1493)
Email: spatial@communications.gov.au
Web: www.anzlic.org.au

Table of Contents

Document Versioning

Date	Version No.	Description	Author
18 Jun 2013	0.1	First draft	Office of Spatial Policy (OSP)
26 Jun 2013	0.2	Clean draft with references to national PSPF and internal DRET Security documentation	OSP
19 Feb 2014	0.3	Update responsibilities to Dept of Communications	Spatial Policy Branch (SPB)
17 Mar 2014	0.4	Contact Officer comments (VIC)	SPB

FSDF– Security

Introduction

1. This document defines the security arrangements that have been established to support the implementation of the Australian and New Zealand Foundation Spatial Data Framework (FSDF). The applicable overarching policy is the Australian Government Protective Security Policy Framework (PSPF)[1]. Where equivalent New Zealand Government security policy applies, acknowledgement will be made in future iterations of this document.

2. The FSDF is a federated project across the Commonwealth governments of Australia and New Zealand and the governments of the States and Territories of Australia therefore the prime responsibility for the security of the project and system(s) that result is with the Australian Government. The Secretary of the Department of Communications has overall responsibility for the protective security policy for the FSDF.

Scope

3. The PSPF is mandatory for Commonwealth agencies and the Commonwealth expects state and territory government agencies that hold or access national security classified information to apply the PSPF, as shown in Figure 1. All agencies involved in the FSDF are expected to develop their own protective security policy and plans.

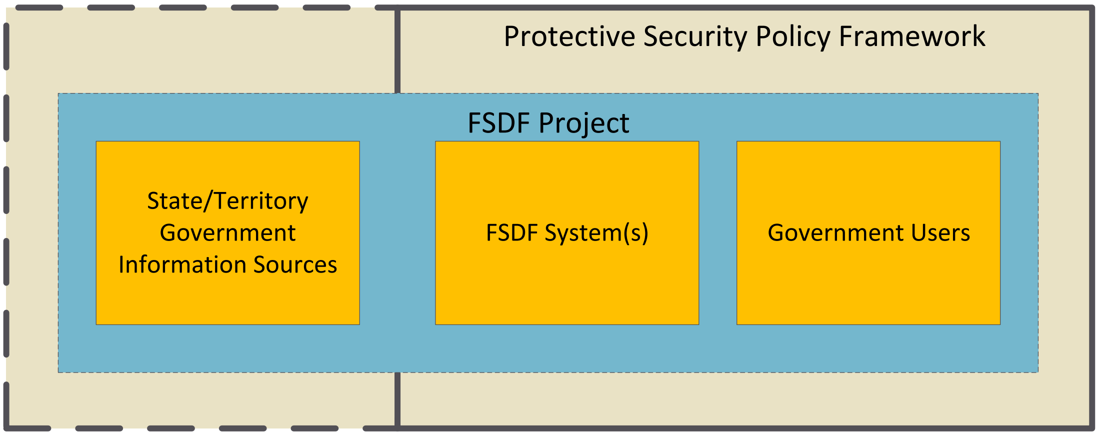
Protective Security Policy Framework
FSDF Project
State/Territory Government Information Sources
FSDF System(s)
Government Users

Figure 1. The FSDF security domain.

[1] The Australian Government Protective Security Policy Framework (PSPF) dated 6 Jun 2010, Attorney-General's Department.

4. This security policy applies to the FSDF as a Department of Communications sponsored project.

Business Context

5. The FSDF is a major conduit for data sourced from local and state government sources, aggregated into national datasets. Information managed through the FSDF will be consumed by Government security accredited systems, including protected systems as shown in Figure 2. Given that much of the information will be sourced from non-Commonwealth government agencies, the FSDF will be the primary tool to bring the information within the control of the PSPF.

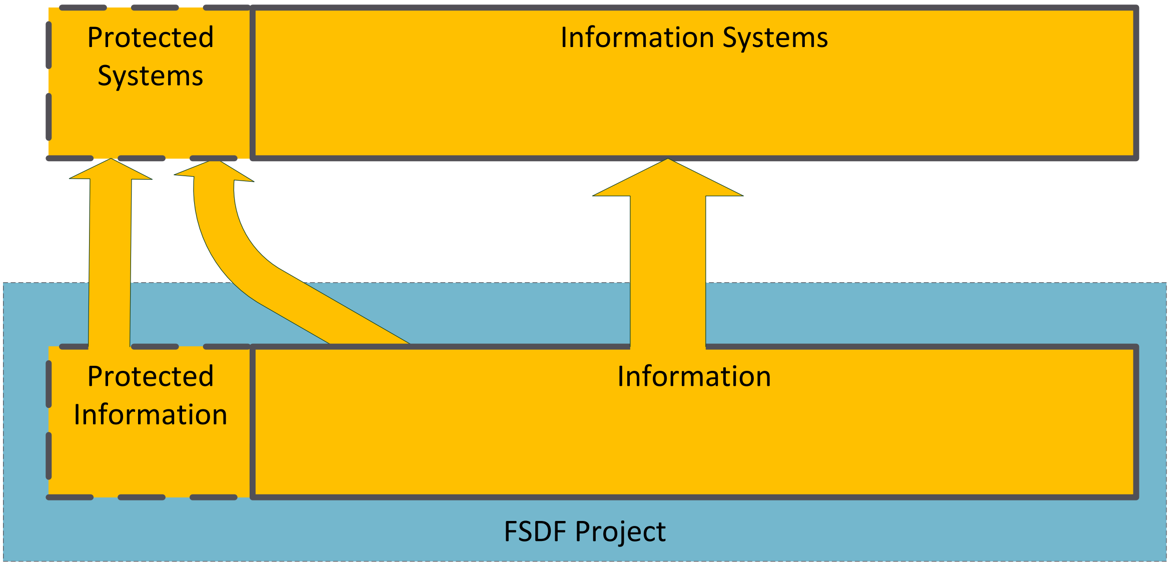

Figure 2. The information flow of the FSDF.

The Australian Government Protective Security Policy Framework

6. The Australian Government needs to be confident that it has measures in place to secure its capacity to discharge its responsibilities. In particular, Australian Government functions and official resources require safeguarding from sources of harm that would weaken, compromise or destroy them. These sources of harm could include threats from criminally or politically motivated individuals or groups, disgruntled employees or foreign intelligence services.

7. An appropriate protective security environment is fundamental, not only to good business and management practice, but ultimately to good government.

8. Protective security measures are usually a combination of physical, personnel, information, and information and communications technology security measures. These measures may be expensive to implement; however, appropriate protective security will enhance an agency’s performance and further its delivery of government objectives.

9. A secure environment is not necessarily a secret environment. Security decisions are no different to other administrative decisions. They must be formulated on a sound factual, financial, lawful and ethical basis and, most importantly, they should be based on an assessment of risk.

10. Agencies that do not provide an appropriate security environment for their functions and official resources place the Australian Government at risk. Any compromise of government functions and objectives has the potential to damage both the public interest and the public's confidence in Australia's democratic institutions.

11. Australia's protective security policy is organised in a tiered, hierarchical structure – the PSPF. This framework has been developed to be read in its entirety following the structure as outlined in the diagram below. Documents are inter linked and should not be read in isolation.

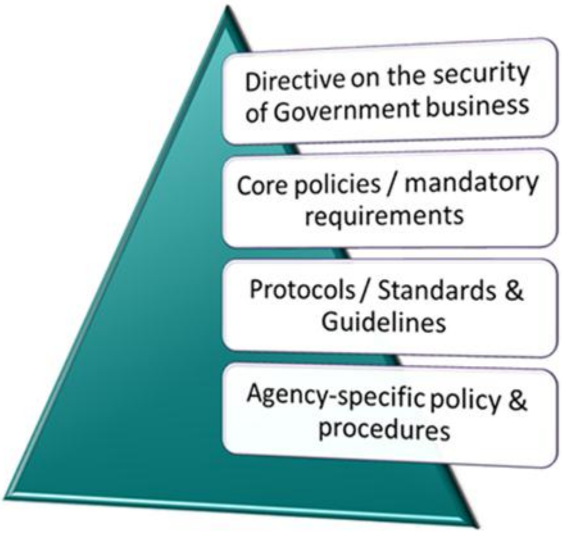
Directive on the security of Government business
Core policies / mandatory requirements
Protocols / Standards & Guidelines
Agency-specific policy & procedures

Figure 3. A representation of the Australian Government Protective Security Policy Framework.

12. The first three levels of the PSPF provide the Australian Government requirements and guidelines, specifying why and how relevant agencies are to comply with the framework. The Agency-specific policy and procedures define the practice and documentation needed to achieve compliance with the framework.

Agency-specific Policy and Procedures

13. Agency- specific documentation[2] covering protective security policies and procedures have been developed by the Department of Communications.. The FSDF sits under this Department policy as a sponsored project and the FSDF System Security Plan specifies the security requirements of the FSDF and subordinate elements. Relevant documentation is;

[2] DBCDE (Department of Communications) Protective security policy dated June 2011.

a. DBCDE (Department of Communications) Protective Security Policy dated June 2011,

b. Department of Communications Security Risk Management Plan,

c. FSDF–Spatial Information Policies–Security (this document), and

d. FSDF System Security Plan.

14. The relationship between these documents within the security framework is depicted in Figure 4 below.

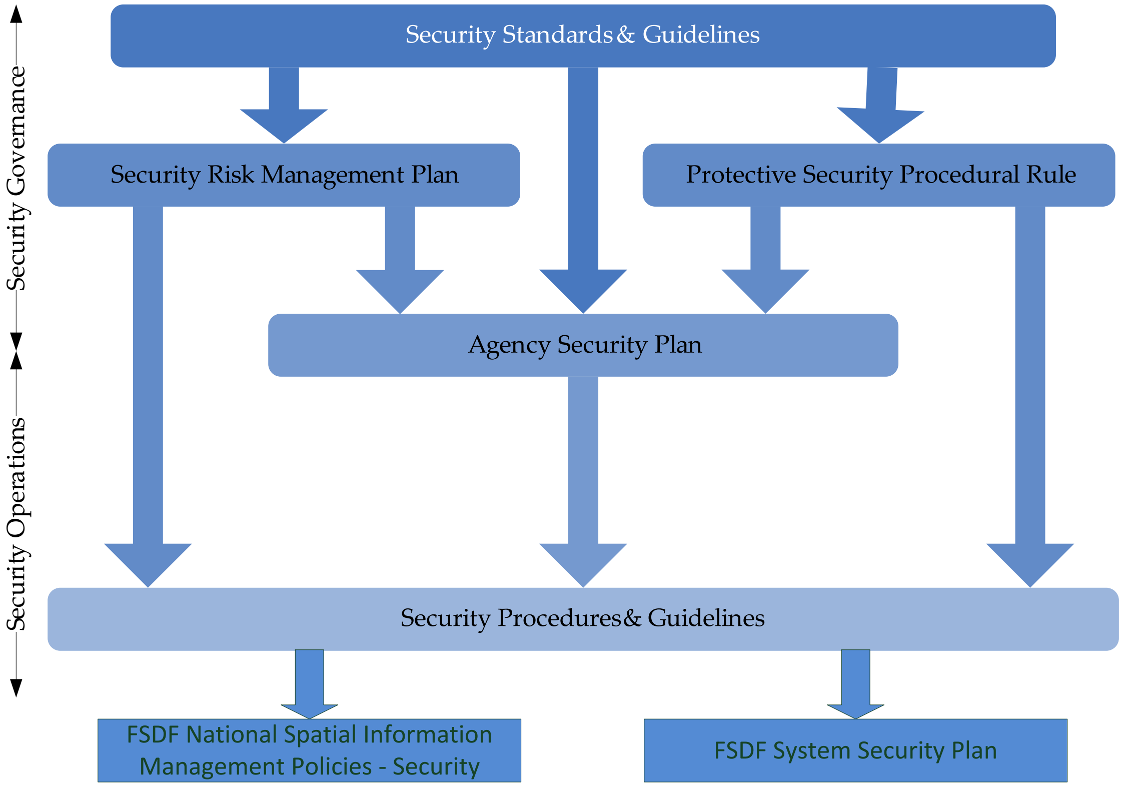
Security Governance
Security Operations
Security Standards & Guidelines
Security Risk Management Plan
Protective Security Procedural Rule
Agency Security Plan
Security Procedures & Guidelines
FSDF National Spatial Information Management Policies - Security
FSDF System Security Plan

Figure 4 - Security framework documentation

15. **DBCDE (Department of Communications) Protective Security Policy dated June 2011.** The security policy defines the overarching security objectives for the Department of Communications.

16. **Department of Communications Security Risk Management Plan.** The Security Risk Management Plan identifies and analyses risks within the Department of Communications context and defines ongoing treatments for the Department of Communications.

17. **FSDF–Spatial Information Policies–Security.** This policy explains the FSDF security arrangements in the context of the PSPF. Because the FSDF is a multi- jurisdictional project and incorporates New Zealand, the security aspects need to be explicit to ensure no weaknesses exist in implementation.

18. **FSDF System Security Plan.** The Security Plan treats the FSDF as a system and defines how the Department of Communications will mitigate identified risks and who is responsible for implementing and maintaining risk mitigation controls defined in the Security Risk Management Plan. The Security Plan describes the security measures for the FSDF and also defines how compliance is maintained for the system. Key components of the Security Plan specified in accordance with the Controls Manual of the Australian Government Information Security Manual[3]and include;

    a. Stakeholders

    b. Controls, and

    c. Compliance.

19. The FSDF System Security Plan is an integral component of all FSDF planning activities and the General Manager, Spatial Policy Branch is responsible for its maintenance in accordance with the Department of Communications guidelines.

Summary

20. The application of the principles and controls in the PSPF should be undertaken within the broader risk management framework for the FSDF.

[3] The Australian Government Information Security Manual (ISM), 2012, Defence Signals Directorate.