



Mr Simon Reardon
Cyber & Information Security Division

Australian Signals Directorate

ICT Evaluation Programs





Australian Signals Directorate

ICT Evaluation Programs

Mr Simon Reardon
Cyber & Information Security Division





INFORMATION SECURITY ADVICE

FOR ALL LEVELS OF GOVERNMENT



Pause ■ ■ ■ ■



2016
Australian Government
Information Security Manual



Top 4
Strategies to Mitigate
Targeted Cyber Intrusions



EPL
Evaluated Products List



Now Recruiting:
Offensive and
Defensive Cyber
Specialists

- 
- Intelligence Services Act, 2001
 - Protective Security Policy Framework
 - Information Security Manual
- 

Intelligence Services Act, 2001

The functions of ASD are:

- (a) to obtain intelligence about the capabilities, intentions or activities of people or organisations outside Australia in the form of electromagnetic energy, whether guided or unguided or both, or in the form of electrical, magnetic or acoustic energy, for the purposes of meeting the requirements of the Government, and in particular the requirements of the Defence Force, for such intelligence; and
- (b) to communicate, in accordance with the Government's requirements, such intelligence; and
- (c) to provide material, advice and other assistance to Commonwealth and State authorities on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means; and**
- (d) to provide assistance to the Defence Force in support of military operations and to cooperate with the Defence Force on intelligence matters; and
- (e) to provide assistance to Commonwealth and State authorities in relation to:**
 - (i) cryptography, and communication and computer technologies;** and
 - (ii) other specialised technologies acquired in connection with the performance of its other functions; and
 - (iii) the performance by those authorities of search and rescue functions; and
- (f) to co-operate with and assist bodies referred to in section 13A in accordance with that section.



- to protect their people, information and assets, at home and overseas.

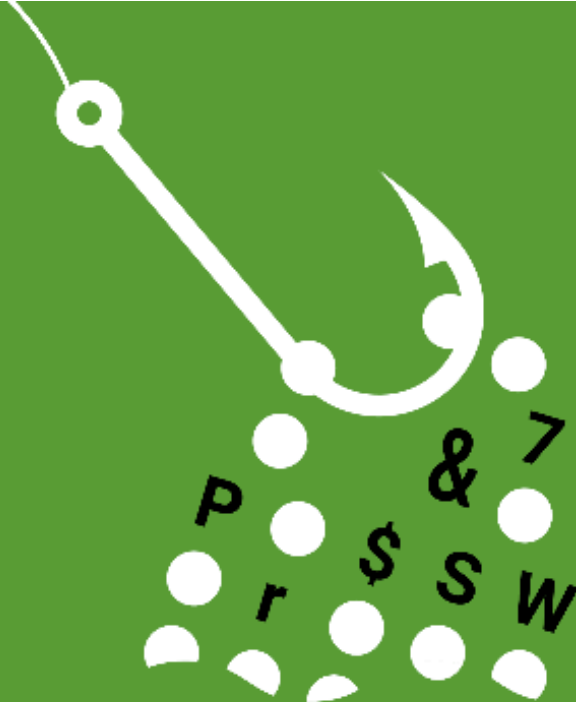
- provides policy, guidance and better practice advice.

- The purpose of the ISM is to assist Australian government agencies in applying a risk– based approach to protecting their information and systems.

- PSPF mandatory requirement INFOSEC 4 requires agencies to implement the Strategies to Mitigate Targeted Cyber Intrusions as outlined in the ISM.

STRATEGIES to MITIGATE CYBER SECURITY INCIDENTS

A NEW CYBER SECURITY BASELINE



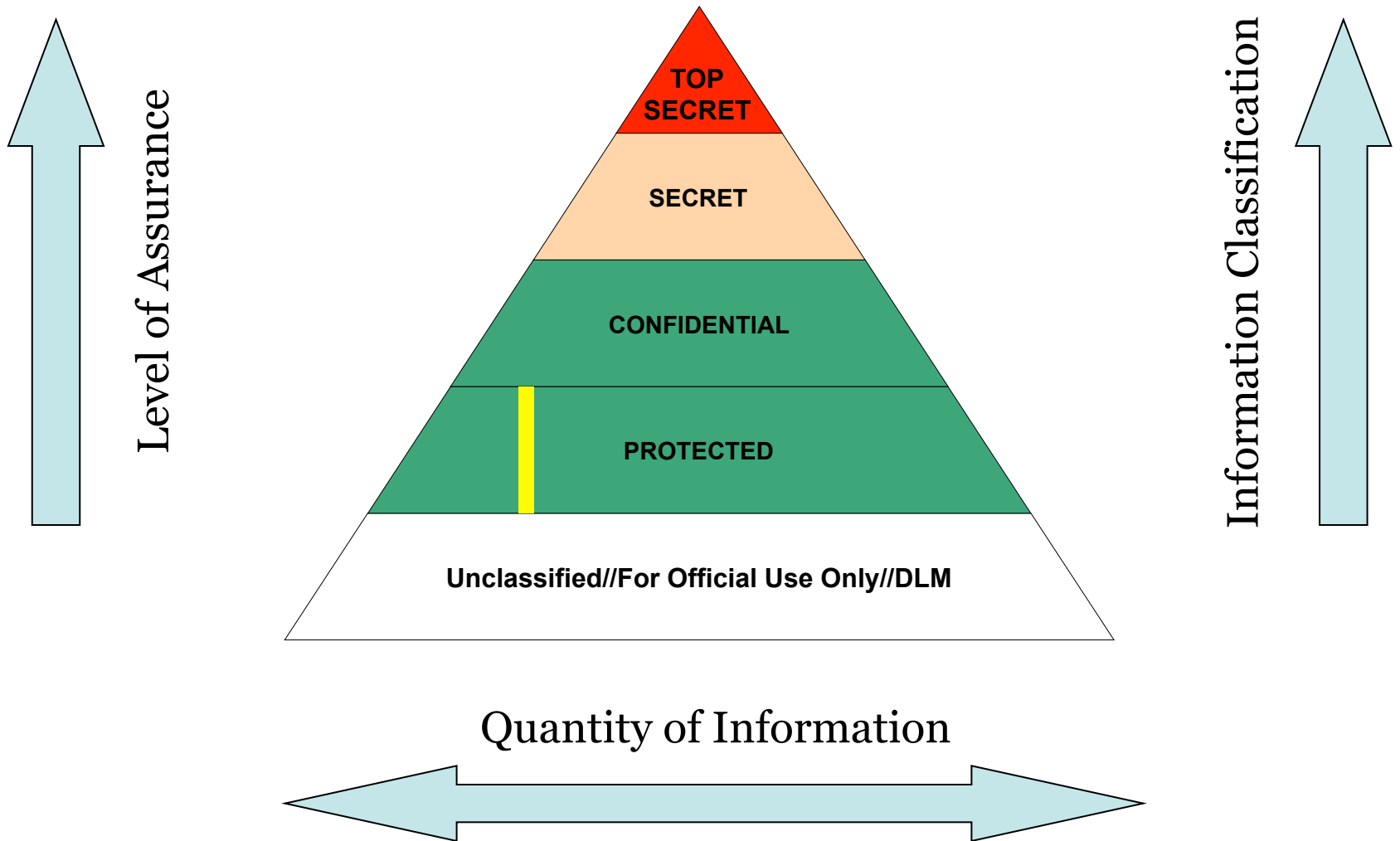
1. Application Whitelisting
 2. Patch Applications
 3. Patch Operating Systems
 4. Restrict Administrative Privileges.
-

1. Attorney-General's Department
2. Department of Agriculture and Water Resources
3. Department of Communications and the Arts
4. Department of Defence
5. Department of Education and Training
6. Department of Employment
7. Department of Finance
8. Department of Foreign Affairs and Trade
9. Department of Health
10. Department of Human Services
11. Department of Immigration and Border Protection
12. Department of Industry, Innovation and Science
13. Department of Infrastructure and Regional Development
14. Department of Social Services
15. Department of the Environment and Energy
16. Department of the Prime Minister and Cabinet
17. Department of Veterans' Affairs
18. Treasury

Commonwealth Agencies

1. ABC – Australian Broadcasting Corporation
2. Aboriginal Hostels Limited
3. Administrative Appeals Tribunal
4. Airservices Australia
5. Anindilyakwa Land Council
6. Army and Air Force Canteen Service
7. Asbestos Safety and Eradication Agency
8. Auditing and Assurance Standards Board
9. Austrade – Australian Trade and Investment Commission
10. Australia Council for the Arts
11. Australia Post
12. Australian Accounting Standards Board
13. Australian Aged Care Quality Agency
14. Australian Antarctic Division
15. Australian Border Force
16. Australian Bureau of Statistics
17. Australian Centre for International Agricultural Research
18. Australian Charities and Not-for-profits Commission
19. Australian Civil-Military Centre
20. Australian Commission for Law Enforcement Integrity
21. Australian Commission on Safety and Quality in Health Care
22. Australian Communications and Media Authority
23. Australian Competition and Consumer Commission
24. Australian Competition Tribunal
25. Australian Criminal Intelligence Commission
26. Australian Curriculum, Assessment and Reporting Authority
27. Australian Egg Corporation Ltd
28. Australian Electoral Commission
29. Australian Energy Regulator

Australian Government Security Classification System



- **Basic Assurance**

- Common Criteria Recognition Arrangement

- Australasian Information Security Evaluation Program (AISEP)

- **Medium Assurance**

- Australian Signals Directorate Cryptographic Evaluation (ACE) – In-house

- **High Assurance**

- Australian Signals Directorate in-house Evaluation

- **Tailored Assurance**

- Australian Signals Directorate in-house Evaluation



Australian Government

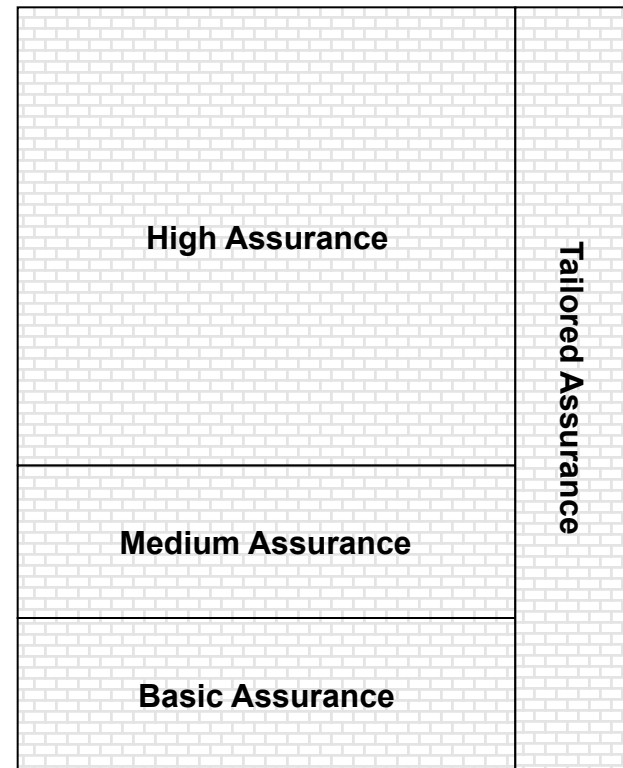
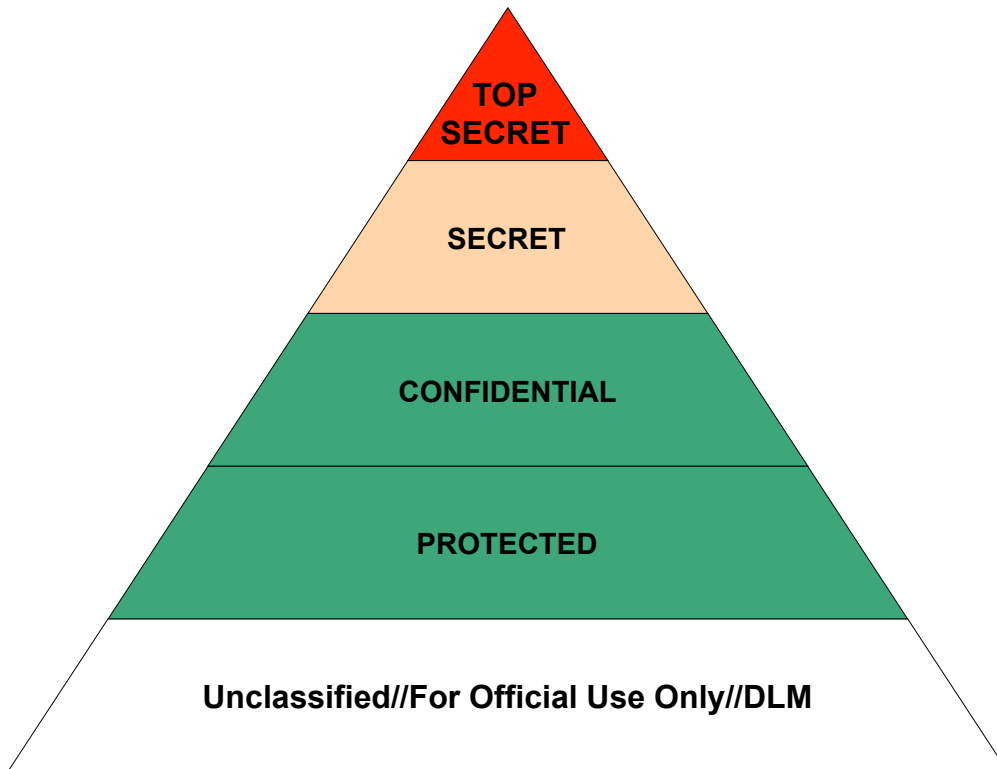


Australian Government



Australian Government

Evaluation Program Mapping



- National PPs
- cPPs
- iTCs

- Position Statements
- Endorsement Statements

Approved Protection Profile List

Technology	Protection Profile	Version	Published
Certification authorities	Certification Authority Protection Profile (PDF)	1.0	December 2015
Data protection	Collaborative Protection Profile for Full Drive Encryption – Authorisation Acquisition (AA cPP) (PDF) AA cPP Supporting Document (PDF)	1.0	May 2016
Data protection	Collaborative Protection Profile for Full Drive Encryption - Encryption Engine (EE cPP) (PDF) EE cPP Supporting Document (PDF)	1.0	May 2016
Network-related devices	Collaborative Protection Profile for Network Devices (ND cPP) (PDF) ND cPP Supporting Document (PDF)	1.0	May 2016
Network-related devices	Collaborative Protection Profile for Network Devices Extended Package Intrusion Prevention Systems (ND cPP IPS EP) (PDF)	2.1	May 2016
Network-related devices	Collaborative Protection Profile for Network Devices Extended Package VPN Gateway (ND cPP VPN GW EP) (PDF)	2.0	May 2016
Network-related devices	Collaborative Protection Profile for Network Devices Extended Package Wireless Local Area Network (WLAN) Access Systems (ND cPP WLAN AS EP) (PDF)	1.0	May 2016
Network-related devices	Collaborative Protection Profile for Stateful Traffic Filter Firewalls (FW cPP) (PDF) FW cPP Supporting Document (PDF)	1.0	May 2016
Network-related devices	Protection Profile for IPsec Virtual Private Network (VPN) Clients (PDF)	1.4	May 2016
Mobility	Protection Profile for Mobile Device Fundamentals (MDF PP) ASD Mandatory Requirements Addendum to MDF PP v2.0 (PDF)	2.0	May 2016

Simon Reardon

Manager, Australasian Information Security Evaluation Program /

Evaluations Program Coordinator

Cyber Security

- The ASD Cryptographic Evaluation process can be described as an unconstrained search for cryptographic vulnerabilities.
- ASD performs this search so that Australian government agencies can rely on the strength and quality of the cryptographic security used to protect classified information and systems.
- The main security functionality analysed during a ACE is confidentiality of data.
- In order for a product to pass a ACE, ASD must have a level of confidence in the security functionality provided by the product and be able to accurately assess strength of function, particularly in regard to confidentiality.

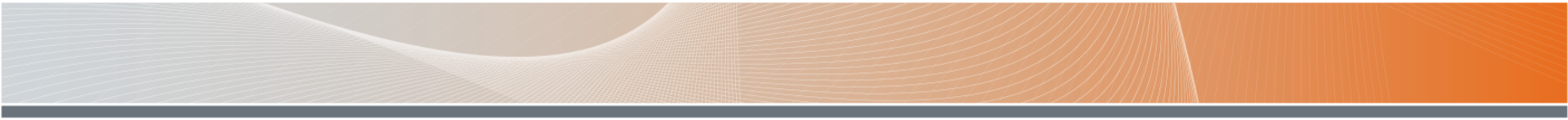
- Data at Rest / Data in Transit

- **Purpose of cryptography**
- The purpose of cryptography is to provide **confidentiality**, integrity, authentication and non– repudiation of information.
- Confidentiality is one of the most common cryptographic functions, with encryption providing protection to information by making it unreadable to all but authorised users.

- **FIPS 140** is not a substitute for an ACE. FIPS 140 is concerned solely with the cryptographic functionality of a module and does not consider any other security functionality.
- Cryptographic evaluations of products will normally be conducted by ASD. Where a product's cryptographic functionality has been validated under FIPS 140, ASD can, at its discretion, and in consultation with the vendor, reduce the scope of an ACE.

- AACA – ASD Approved Crypto Algorithm - Information at rest is protected by an AACA.

- AACP – ASD Approve Crypto Protocol - Information in transit is protected by an AACPimplementing AACAs.

- 
- FIPS 140 is not a substitute for an ACE. FIPS 140 is concerned solely with the cryptographic functionality of a module and does not consider any other security functionality.
 - Cryptographic evaluations of products will normally be conducted by ASD. Where a product's cryptographic functionality has been validated under FIPS 140, ASD can, at its discretion, and in consultation with the vendor, reduce the scope of an ACE.
- 