+61 2 6100 0464
NJOY SECURITY, PO Box 176, Bungendore, NSW, 2621
info@njoysecurity.com
au.linkedin.com/in/nathanjoy/

Mr. Chad Woolf
Director, AWS Risk & Compliance
Amazon Web Services
440 Terry Ave N, Seattle, WA 98109

20 October 2014

Amazon IRAP Assessment – Letter of Compliance

Dear Mr. Woolf,

This document is to act as a letter of compliance for Amazon Web Services.

From January through October 2014 NJOY SECURITY was engaged to conduct an IRAP assessment of Amazon Web Services, in accordance with the process prescribed in the Australian Government Information Security Manual (ISM) and Protective Security Policy Framework.

The IRAP assessment was undertaken by Nathan Joy, who is an Australian Signals Directorate endorsed assessor under the Information Security Registered Assessors Program (IRAP). Amazon Web Services was assessed with regard to the Australian Government requirements for unclassified but sensitive information referred to as UNCLASSIFIED (DLM). Unclassified (DLM) requirements are identified in the ISM as Government system (G) controls.

The scope of the IRAP assessment included the following Amazon services and facilities:

- The Amazon EC2, VPC, S3 & EBS services hosted in the Asia Pacific (Sydney) Region;
- Amazon's Australian Data Centre Facilities.

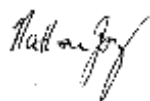NJOY SECURITY conducted the IRAP assessment in two audit stages:

- The first stage audit determined whether the system architecture (including information security documentation) was based on sound security principles and had addressed all applicable controls from the ISM.
- The second stage audit determined whether the controls had been implemented and were operating effectively. The process included inspections of premises, personnel interviews, process demonstrations, configuration reviews and the review of certification reports which included evidence of control validation.

NJOY SECURITY have reviewed the Amazon Web Service System Security Plan and have prepared a Report of Compliance which records the applicability and compliance with specific ISM controls. A summary of the IRAP assessment findings is provided in the attached table.

The IRAP assessor's finding is that the applicable ISM controls relating to the processing, storage and transmission of UNCLASSIFIED (DLM) Australian Government data within Amazon's Asia Pacific (Sydney) Region have been implemented and are operating effectively.

Amazon should advise an IRAP assessor of any significant future changes to the services, which might influence the effectiveness of the implemented ISM controls. Amazon should remain informed of future releases of the Australian Government Information Security Manual, which may include control changes which may affect Amazons compliance.

Regards,

Nathan Joy, BLS (Criminology), DipGov (Fraud Control), DipGov (Investig.), DipGov (Intel.), ISO27001 Lead Auditor, CISSP, IRAP Assessor
Principle Security Consultant, NJOY SECURITY
Recipient of the SANS 2012 National Cybersecurity Innovation Award

+61 2 6100 0464
NJOY SECURITY, PO Box 176, Bungendore, NSW, 2621
info@njoysecurity.com
au.linkedin.com/in/nathanjoy/

ISM Chapter	Control Effectiveness			Statement of Control Effectiveness
	Effective	Partially Effective	Not Effective	
Information Security Risk Management				
Risk Assessment	✓			NJOY SECURITY has assessed Amazons risk management controls to be effective for the management of Amazon information security risks.
Security Risk Management Plan	✓			
Role & Responsibilities				
Chief Information Security Officer	✓			NJOY SECURITY has assessed that the roles defined by Amazon meet the intent of the roles described within the ISM.
IT Security Advisor	✓			
IT Security Manager	✓			
IT Security Officer	✓			
System Owner	✓			
System Users	✓			
Information Security Documentation				
Documentation Framework	✓			Amazons has established Information Security Policies which provide clear policy guidance and are assessed to be effective.
Information Security Policy	✓			
System Security Plan	✓			The Amazon SSP properly documents security controls for AWS systems and is assessed to be effective.
Standard Operating Procedures	✓			The Amazon Standard Operating Procedures address all applicable security controls and are considered to meet the intent of the applicable controls within the ISM.
Incident Response Plan	✓			Amazons Incident Response Plan & Procedures meet the ISM requirements and are assessed to be effective.

+61 2 6100 0464
NJOY SECURITY, PO Box 176, Bungendore, NSW, 2621
info@njoysecurity.com
au.linkedin.com/in/nathanjoy/

ISM Chapter	Control Effectiveness			Statement of Control Effectiveness
	Effective	Partially Effective	Not Effective	
Business Continuity and Disaster Recovery Plan	✓			Business continuity and disaster recovery controls have been appropriately addressed by Amazon in manner which meets the requirements of the ISM.
Information Security Monitoring				
Vulnerability Management	✓			Amazons vulnerability management practices are assessed as effective and meet the requirements of the ISM.
Change Management	✓			Amazons change management policy and processes are assessed as being effective and meet the requirements of the ISM.
Cyber Security Incidents				
Detecting, Reporting and Managing Cyber Security Incidents	✓			Amazons cyber security incident detection, reporting, management and policies & processes are effective and meet the requirements of the ISM.
Physical & Environmental Security				
Physical Security for Systems	✓			Amazons physical security controls are fully effective and are assessed to exceed the ISM requirements for storage of UNCLASSIFIED (DLM) data.
Personnel Security for Information Systems				
Information Security Awareness & Training	✓			The IRAP Assessor audited Amazons personnel security measures and interviewed security personnel. Amazons personnel security controls are assessed to be fully effective and meet the requirements of the ISM.
Authorisations, Security Clearances & Briefings	✓			
Communications Security				
Communications Security	✓			Communications security within Amazons data centres is assessed to be effective in meeting the

+61 2 6100 0464
NJOY SECURITY, PO Box 176, Bungendore, NSW, 2621
info@njoysecurity.com
au.linkedin.com/in/nathanjoy/

ISM Chapter	Control Effectiveness			Statement of Control Effectiveness
	Effective	Partially Effective	Not Effective	
	✓			intent of the applicable ISM controls relating to communication security.
Product Security				
Product Security	✓			The IRAP assessor concluded that Amazon securely select, acquire, install, configure, label, maintain, repair, sanitise and dispose of ICT products in manner which meets the requirements of the ISM.
Media Security				
Media Security	✓			Amazons physical security controls are fully effective and are assessed to exceed the ISM requirements for secure management of UNCLASSIFIED (DLM) media.
Asset Management	✓			Amazons asset management policies and procedures are assessed to be fully effective and meet the requirements of the ISM.
Software Security				
SOE	✓			Amazons operating system security controls are assessed to be fully effective and meet the requirements of the ISM.
Application Whitelisting	✓			Amazons application whitelisting controls meet the intent of the ISM for the control of permitted binaries.
Software Application Development	✓			Amazons management of software development activities are fully effective and are assessed to meet the ISM requirements.
Access Control				
Privileged Access	✓			Amazons privileged access security controls are assessed to be fully effective and meet the requirements of the ISM.
Event Logging and Auditing	✓			Amazons event logging and auditing controls are fully effective and are assessed to meet the ISM requirements.

+61 2 6100 0464
NJOY SECURITY, PO Box 176, Bungendore, NSW, 2621
info@njoysecurity.com
au.linkedin.com/in/nathanjoy/

ISM Chapter	Control Effectiveness			Statement of Control Effectiveness
	Effective	Partially Effective	Not Effective	
Secure Administration				
Secure Administration	✓			Amazons secure administration controls are fully effective and are assessed to meet the ISM requirements.
Network Security				
Network Management, Design and Configuration	✓			Amazons network management and configuration controls are fully effective and are assessed as meeting the ISM requirements for the transmission and handling of UNCLASSIFIED (DLM) data.
Ensuring Service Continuity	✓			Amazon has implemented effective DDoS controls which are assessed to meet the ISM requirements for ensuring service continuity.
Intrusion Detection and Prevention	✓			Amazon has implemented DDoS controls that are effective and are assessed to meet the intent of the ISM requirements for ensuring intrusion prevention, detection and response.
Cryptography				
Cryptographic Security	✓			The cryptographic security implemented by Amazon is considered to be an effective security control.
Cross Domain Security				
Cross Domain Security	✓			The firewalling capability implemented within Amazon is assessed to be effective for the protection of UNCLASSIFIED (DLM) information.
Data Transfers				
Data Transfers	✓			Amazon has established security mechanisms for data transfer which meet the intent of the ISM and are assessed to be effective for the transfer of UNCLASSIFIED (DLM) information.