Address: Po Box 176 Bungendore, NSW, 2621
Email: irap@njoysecurity.com.au

9 November 2020

In 2020, Zscaler engaged NJOY SECURITY to conduct an IRAP Assessment of its Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) services.

As required by the Information Security Manual (ISM), NJOY SECURITY completed a Phase 1a IRAP Assessment of ZIA and ZPA. In the Phase 1a IRAP Assessment, Zscaler's security fundamentals and the in-scope ZIA and ZPA cloud services were assessed by the IRAP assessor. The objective of the Zscaler security fundamentals assessment was to assess and document the security practices and posture of Zscaler itself. This is so cloud consumers can determine if Zscaler itself is operating securely and producing secure cloud services, and is suitable for handling the cloud consumer's data.

The other part of the Phase 1a assessment focused on the Zscaler ZIA and ZPA cloud services that are in scope of the assessment. These cloud services were assessed against the applicable "Official" ISM security controls, so cloud consumers can determine the security risks of using Zscaler's cloud services.

The Phase 1a Zscaler IRAP Assessment has been completed and it validated that Zscaler has:

- identified all applicable "Official" controls from the June 2020 ISM;
- developed appropriate policies which support the protection of "Official" information that is processed, stored or communicated by the ZIA and ZPA services;
- developed many of the documents specified by the ISM;
- Identified instances on non-compliance with ISM requirements.

The IRAP Assessor has documented the results of the Phase 1a IRAP Assessment in the Zscaler IRAP Assessment Report. Zscaler is actively developing its *Plan of Action and Milestones* (POAM) which is a requirement post completion of a Phase 1a IRAP Assessment. Australian organisations and Government agencies who choose to consume ZIA and ZPA services should ensure they align with the requirements of the ACSC *Anatomy of a Cloud Assessment and Authorisation* document (specifically Phases 1c, 2a and 2b).

NJOY SECURITY advises Australian Government agencies (Federal, State & Local), Universities and Research Organisations, Resource, Energy & Critical Infrastructure Sectors and businesses involved in the defence supply chain to:

- refer to the Australian Security Intelligence Organisation (in particular the Business and Government Liaison Unit) for assistance managing any national security risks associated with their intended use case;
- refer to the Critical Infrastructure Centre for assistance managing any critical infrastructure risks associated with their intended use case;
- Undertake the requisite due diligence if they elect to use ZIA or ZPA services, noting that they must develop an Authorisation Package and grant the solution Authority to Operate;
- share their Authorisation Package with other interested organisations and agencies (including ACSC) in order to create baselines for re-use so as to increase the capacity of government to undertake assessments, whilst also strengthening security outcomes;
- Undertake due diligence for their ICT systems that connect to Zscaler ZIA and/or ZPA which includes aligning with ACSC guidance provided in ACSC publications and the ISM; and
- seek guidance from the ACSC in relation to any Zscaler specific risks.

DocuSigned by:
Nathan Joy
FE0D85DFDCAC459...

Mr. Nathan Joy
IRAP Assessor - 1037
NJOY SECURITY
irap@njoysecurity.com.au