SHEARWATER™
securing your information

Rose Quijano-Nguyen
Director of Security and Certifications Programs
Citrix, Inc
4988 Great America Parkway
Santa Clara, CA 95054

October 12, 2020

Citrix Workspace Information Security Registered Assessors Program (IRAP) Assessment

Dear Ms Quijano-Nguyen,

At the request of Citrix, Michael Farlow, an Australian Signals Directorate (ASD) registered IRAP Assessor[1], on behalf of Shearwater Solutions, conducted an IRAP[2] assessment of *Citrix Workspace* against the PROTECTED controls within the Australian Government *Information Security Manual* (ISM). The assessment was undertaken between May and September of 2020 during the COVID-19 global pandemic. As a consequence, the assessment did not include site visits. Instead, virtual meetings and video conferences were conducted to interview Citrix personnel and to observe security control implementation.

The products and services in scope of the review are summarised as: 'Citrix Workspace incorporating Citrix Virtual Apps and Desktops Service, Citrix Gateway Service (HDX Proxy), Citrix Cloud Platform and Citrix Identity Platform'. Citrix Workspace is hosted within Microsoft Azure East and South-East Australian datacentre regions and inherits controls from previous Azure IRAP assessments[3], including physical infrastructure, security software, database management systems, and network, ICT equipment and media management.

Citrix Workspace consumes 16 Azure services, all of which have been IRAP assessed at the PROTECTED classification level.

Based on Citrix corporate documentation, Citrix Workspace system security documentation and observations made during the IRAP assessment, Citrix Workspace is compliant with the majority of applicable ISM controls. A summary of assessment results against each chapter of the ISM is outlined within Table 1.

Regards,

Michael Farlow
IRAP Assessor | Shearwater
www.shearwater.com.au

[1] ASD Registration Number 1186
[2] https://www.cyber.gov.au/acsc/view-all-content/programs/irap
[3] https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-ccsl-irap-australia?view=o365-worldwide

Table 1: ISM Implementation Summary

ISM Section	Summary of Findings
Cyber security roles	All applicable controls in this section are implemented or not applicable.
Authorising systems	All applicable controls in this section are implemented or not applicable.
Cyber security incidents	All applicable controls in this section are implemented or not applicable.
Outsourcing	All applicable controls in this section are implemented or not applicable.
Security documentation	All applicable controls in this section are implemented or not applicable.
Physical security	All applicable controls in this section are implemented or are inherited from Azure.
Personnel security	Citrix personnel are globally dispersed, with the majority based in the USA. Consequently, these internationally-based personnel do not hold Australian national security clearances. Citrix mitigate the risk associated with this by ensuring that only approved Citrix personnel have access to cloud service environments that host customer data. Additionally, personnel do not have access to customer data or the immediate environments which host this data. Personnel also undergo pre-employment onboard vetting while all access to Citrix Workspace is centrally logged and monitored. Citrix implement additional controls to limit when and how access to the system by its personnel occurs.
Communications infrastructure	All applicable controls in this section are inherited from Azure.
Communications systems	No controls within this section are applicable to the system.
Enterprise mobility	No controls within this section are applicable to the system.
Evaluated products	All applicable controls in this section are inherited from Azure.
ICT equipment management	No controls within this section are applicable to the system.
Media management	All applicable controls in this section are implemented or are inherited from Azure.
System hardening	Citrix utilises soft token based Multifactor Authentication (MFA) for all personnel. Citrix Workspace customers are able to implement MFA for their personnel if they choose.
System management	The current Citrix patch strategy adopts a risk-based approach with defined remediation timeframes. These timeframes currently exceed those detailed in the ISM. The IRAP assessment includes recommendations for Citrix to align its strategy with the ISM patching timeframes.
System monitoring	Citrix's approach to log retention is driven by requirements under the EU General Data Protection Regulation Act, which limits the duration in which organisations can retain information. Consequently, event, DNS and proxy logs are stored for 12 months.
Software development	All applicable controls in this section are inherited from Azure.
Database systems management	All applicable controls in this section are inherited from Azure.
Email management	Citrix Workspace does not provide functionality for users to send or receive emails. The system can generate outbound email notifications to users; however, these do not carry protective markings in line with the Australian Government Security Classification Scheme. All other applicable controls are implemented or not applicable.
Network management	All applicable controls in this section are implemented or are inherited from Azure.

ISM Section	Summary of Findings
Using cryptography	Citrix implements TLS 1.2 throughout its system for all HTTPS based connections. TLS 1.3 is currently not utilised due to compatibility and support issues with Microsoft operating systems. All other applicable controls are implemented or not applicable.
Gateway management	Citrix personnel with access to system gateways do not hold Australian national security clearances. Citrix mitigate the risk associated with this in the manner described within the *Personnel security* section. Citrix does not deploy an evaluated firewall between the Citrix Workspace system and public infrastructure. Citrix utilises Azure Load Balances and Network Security Groups (NSG) to monitor, filter and block traffic entering and leaving the system. There are currently no Common Criteria[4] or Australian Signals Directorate (ASD) Cryptographic Evaluated software firewall products in use.
Data transfers and content filtering	All applicable controls in this section are implemented or not applicable.

[4] https://www.commoncriteriaportal.org