



Schellman & Company, LLC
4010 W Boy Scout Boulevard
Suite 600
Tampa, Florida 33607

Tel: 1.866.254.0000

Fax: 1.866.971.7070

Zscaler, Inc.
110 Rose Orchard Way
San Jose, California 95134

August 7, 2019

RE: ENGAGEMENT SUMMARY FOR CJIS

To Whom It May Concern:

I would like to confirm that Schellman & Company, LLC (Schellman) was engaged to perform an assessment of Zscaler Cloud Solutions' controls for protecting information using the requirements from the Criminal Justice Information Services Security Policy v5.8, commonly referred to as CJIS. The CJIS requirements assessed included only SaaS requirements mapped to controls that were also part of the Zscaler Internet Access ("ZIA") and Zscaler Private Access ("ZPA") FedRAMP initial assessments in 2018.

The results of the assessment were provided to Zscaler with the findings summarized in Appendix A of this letter.

Please be advised that this letter summarizes services and deliverables Schellman provided for the sole benefit of Zscaler and Schellman assumes no liability to any third party related to those services, deliverables, or the contents of this letter. Furthermore, all express or implied conditions, representations, and warranties including, without limitation, any implied warranty or condition of merchantability, fitness for a particular purpose, satisfactory quality, accuracy of information content, or arising from usage, are expressly disclaimed by Schellman.

Please notify Zscaler if you require any further information.

Sincerely,

A handwritten signature in black ink that reads "Douglas W. Barbin".

Douglas W. Barbin
Principal

About Schellman

Schellman & Company, LLC is a leading provider of attestation and compliance services. We are the only company in the world that is a [CPA firm](#), a globally licensed [PCI Qualified Security Assessor](#), an [ISO Certification Body](#) and a [FedRAMP 3PAO](#). Renowned for expertise tempered by practical experience, Schellman's professionals provide superior client service balanced by steadfast independence. Our approach builds successful, long-term relationships and allows our clients to achieve multiple compliance objectives using a single third party assessor.

Schellman serves hundreds of clients each year, including many Fortune 1000 and publicly traded companies. For further information, please visit <http://www.schellman.com/>.

Appendix A – Summary Findings

Summary Table

The below table documents the status and applicability of each CJIS Security Policy SaaS requirement to the ZPA and ZIA systems as defined in the CJIS Requirements Companion Document and tested during the FedRAMP Moderate initial assessments. The status legend is as follows:

- “I” indicates the policy area requirements are in place
- “N” indicates the policy area requirements are not in place
- “P” indicates the policy area requirements are partially in place
- “N/A” indicates the policy area requirements are not applicable
- “NT” indicates the policy area requirements were not tested due to scoping (i.e., not included in the FedRAMP control selection defined above)

Policy Area	Policy Area Subsection	Status	Policy Area	Policy Area Subsection	Status
Policy Area 1: Information Exchange Agreements	5.1.1.5	NT	Policy Area 7: Configuration Management	5.7.1.1	I
Policy Area 2: Security Awareness Training	5.2.1	I		5.7.1.2	I*
	5.2.1.1	I		5.7.2	I
	5.2.1.2	I*	Policy Area 8: Media Protection	5.8.1	I
	5.2.1.3	I*		5.8.2.1	I
	5.2.1.4	I		5.8.3	I
	Policy Area 3: Incident Response	5.2.2	NT	Policy Area 9: Physical Protection	5.9
5.2.3		I	5.9.1.1		I*
5.3		I*	5.9.1.2		I
5.3.1		I*	5.9.1.3		I
5.3.2		I	5.9.1.4		I
5.3.2.1		I	5.9.1.5		I
5.3.2.2		I	5.9.1.6		I
5.3.3	I	5.9.1.7	I		
Policy Area 4: Auditing and Accountability	5.3.4	I	5.9.1.8	I	
	5.4	I	5.9.2	I	
	5.4.1	I	Policy Area 10: System and Communications Protection and Information Integrity <i>(Cont.)</i>	5.10.1	I
	5.4.1.1	I		5.10.1.1	I
	5.4.1.1.1	I		5.10.1.2.1	I
	5.4.2	I		5.10.1.2.2	I*
	5.4.3	I		5.10.1.2.3	N/A
	5.4.4	I		5.10.1.3	I
	5.4.5	I		5.10.1.4	N/A
	5.4.6	I		5.10.1.5	I
5.4.7	I	5.10.2		N/A	

Policy Area	Policy Area Subsection	Status	Policy Area	Policy Area Subsection	Status	
Policy Area 5: Access Control	5.5.1	I	(Cont.) Policy Area 10: System and Communications Protection and Information Integrity	5.10.3.1	I	
	5.5.2	I		5.10.3.2	I*	
	5.5.2.1	I		5.10.4.1	I	
	5.5.2.2	I		5.10.4.2	I	
	5.5.2.3	I*		5.10.4.3	I	
	5.5.2.4	I		5.10.4.4	I	
	5.5.3	I		5.12.2	I*	
	5.5.4	I	Policy Area 12: Personnel Security	5.12.3	NT	
	5.5.5	I	5.12.4	I		
	5.5.6	I				
	5.5.6.1	I				
	5.5.6.2	I				
	Policy Area 6: Identification and Authentication	5.6	I			
		5.6.1	I			
5.6.2.1		I				
5.6.2.1.1		I				
5.6.2.1.1.1		I				
5.6.2.1.1.2		NT				
5.6.2.1.2		N/A				
5.6.2.1.3		I				
5.6.2.2		I				
5.6.2.2.1		NT				
5.6.3		I				
5.6.3.1		I				
5.6.3.2		I				
5.6.4	I					

* At least one subcomponent of this requirement had a status of NT; however, other components were tested, and the status is noted.

It is also noteworthy that certain physical and environment controls for ZPA were the responsibility of AWS.