schellman

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

Tel: 1.866.254.0000
Fax: 1.866.971.7070

Zscaler, Inc.
120 Holger Way
San Jose, California 95134

February 7, 2025

RE: ENGAGEMENT SUMMARY FOR ITAR

To Whom It May Concern:

I would like to confirm that Schellman Compliance, LLC (Schellman) was engaged to perform an assessment of Zscaler Cloud Solutions' controls for protecting information using the requirements from the related to aspects of the International Traffic in Arms Regulations ("ITAR"), as of February 7, 2025.

The scope of the review is limited to the personnel screening and authorization management procedures for the Zscaler environments. ZPA Moderate user scope is limited to Zscaler Federal customer support personnel. The specific control activities included within the scope of this engagement can be found in Section 4 of this document. Specifically, testing was performed to confirm the suitability of the design of the controls related to each of the assertions within the Agreement, as described in Section 4 ("Personnel Screening and Authorization Controls").

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,

Douglas W. Barbin
National Managing Principal

About Schellman

"Schellman" is the brand name under which Schellman & Company, LLC and Schellman Compliance, LLC provide professional services. Schellman provides compliance and certification services to a variety of companies, including HITRUST certifications, PCI assessments, FedRAMP assessments, attest examinations (SOC 1, SOC 2, SOC 3), Penetration Testing services, ISO 27001, 27701, 9001, 20000, and 22301certifications, GDPR, CCPA and MS DPR examinations, and several other types of compliance assessments. Schellman & Company, LLC and Schellman Compliance, LLC practice as an alternative practice structure in accordance with the AICPA Code of Professional Conduct and applicable law, regulations, and professional standards. Schellman & Company, LLC is a licensed certified public accounting firm (Florida license number AD62941) registered with the Public Company Accounting Oversight Board (PCAOB) that provides attest services to its clients, and Schellman Compliance, LLC provides nonattest cybersecurity and compliance professional services to its clients. Schellman Compliance, LLC is not a licensed CPA firm. Schellman & Company, LLC and Schellman Compliance, LLC are independently owned and are not liable for the services provided by any other entity providing services under the Schellman brand. Our use of the terms "our firm" and "we" and "us" and terms of similar import, denote the alternative practice structure conducted by Schellman & Company, LLC and Schellman Compliance, LLC.

ITAR Personnel Screening and Authorization Management Requirements

The International Traffic in Arms Regulations ("ITAR", 22 CFR 120-130) implements the 22 U.S.C. 2778 of the Arms Export Controls Act (AECA). ITAR regulates the import and export of arms, munitions, and other "defense articles" as defined on the ITAR U.S. Munitions List. Key terms and requirements relevant to personnel screening and authorization management include the following:

- Technical Data – ITAR defines technical data as "Information, other than software as defined in §120.10(a)(4), which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles" (22 CFR §120.10).
- U.S. Persons – ITAR defines U.S. person as a person who is a lawful permanent resident of the United States which includes U.S. Citizens. It also includes corporations and/or government entities such that permanent residents that work for foreign corporations or governments may not meet the requirements to be a U.S. person (22 CFR §120.15).

Reference is made to the U.S. State Departments website for specific requirements for ITAR –
http://pmddtc.state.gov/regulations_laws/itar.html

No additional subject matter or requirements for compliance with ITAR, including but not limited to the guidelines set for by the Directorate of Defense Trade Controls (DDTC) are covered by this report.

Personnel Screening and Authorization Management Procedures

Procedures

Pre-Employment Screening

Zscaler maintains documented policies and procedures for the screening of new hires and personnel requiring access to the Zscaler environments. Background investigations and identity and employment authorizations are utilized by human resources (HR) personnel to screen candidates and new hires. Citizenship or residency status is verified utilizing the E-Verify program from the U.S. Citizenship and Immigration Services.

When access to the Zscaler environments is required, employees are verified using the I-9 program to confirm citizenship or residency status.

Security Awareness and Training

Zscaler maintains documented policies and procedures for security awareness and training required to be completed for all new hires and personnel requiring access to the Zscaler environments. Security awareness training materials focus on the handling of sensitive federal data, which includes ITAR. Zscaler personnel complete trainings via the Learning Management System (LMS) and training records are maintained for at least a year.

Zscaler Access Authorization

Personnel requiring access to the Zscaler environments are required to submit an access request through the ticketing system with the following approval routings:

- The employee's direct manager to confirm business need and access levels.
- The HR department who confirms that the employee is both a U.S person, I-9 forms completed, security awareness training conducted, and a third-party background check performed.

Once approved logical access is granted to the user based on their role as outlined in the separation of duties matrices. Account reviews of privileged users who possess Zscaler environments access are reviewed on a monthly basis.

Specific Control Activities

The description of Schellman Compliance, LLC's tests of the suitability of design and the results of those tests are also presented in the below Testing Matrices.

Personnel Screening and Authorization Management Controls

#	Control Activity Specified by Zscaler	Test Applied	Test Results
Personnel Screening Procedures			
1.	Documented policies and procedures are in place to guide personnel in the screening of new hires for citizenship or residency status.	Inspected the employee screening policies and procedures to determine that documented policies and procedures were in place to guide personnel in the screening of new hires for citizenship or residency status.	No exceptions noted.
2.	Third-party software is utilized to confirm citizenship or residency status for new hires via the E-Verify program of the U.S. Citizenship and Immigration Services.	Inquired with authorized Zscaler Human Resource representatives regarding the citizenship and residency status validation process to determine that third-party software was utilized to confirm the citizenship or residency for new hires via the E-Verify program of the U.S. Citizenship and Immigration Services.	No exceptions noted.
		Observed the third-party software application and the verification results for a sample of users with access to the Zscaler environments (ZPA High, ZIA High, ZPA Moderate, ZIA Moderate) to determine that third-party software was utilized to confirm citizenship or residency status for new hires via the E-Verify program of the US Citizenship and Immigration Services for each user sampled.	No exceptions noted.
Security Awareness and Training			
3.	Personnel with access to customer environments are required to undergo a specific security awareness and training course for handling sensitive information.	Inspected the security awareness training policies and procedures and the security awareness training content to determine that personnel with access to the Zscaler environments undergo security awareness and training specific to handling sensitive data.	No exceptions noted.
		Inspected the security awareness completion records for a sample of users with access to the Zscaler environments to determine that personnel with access were required to undergo a specific security awareness and training course for handling sensitive information for each user sampled.	No exceptions noted.

#	Control Activity Specified by Zscaler	Test Applied	Test Results
Authorization Management			
4.	Documented policies and procedures are in place for granting access to the Zscaler environments.	Inspected the access control policies and procedures to determine that documented policies and procedures were in place for granting access to the Zscaler environments.	No exceptions noted.
5.	Personnel request access to the Zscaler environments through Zscaler's workflow management system.	Inspected tickets for a sample of users requesting access to the Zscaler environments during the review period to determine that prior to the users gaining logical access tickets were created in the workflow management system in support of approvals and validation of citizenship.	No exceptions noted.
6.	Access requests to the Zscaler environments are approved by the following roles: · Direct Manager	Inspected the access request tickets for a sample of users requesting access to the Zscaler environments during the review period to determine that the access tickets were approved by the following roles: · Direct Manager	No exceptions noted.
7.	The user's direct manager approves access to the Zscaler environments only when citizenship or residency has been confirmed, and the security awareness training program has been completed.	Inspected the access request tickets for a sample of users requesting access to the Zscaler environments to determine that approval was documented by the user's direct manager.	No exceptions noted.
		Inspected the access request tickets, evidence of I-9 verification, and security awareness and training to determine that approval was only granted when citizenship or residency has been confirmed and the security awareness training program has been completed.	No exceptions noted.
8.	Zscaler performs quarterly access reviews of the Zscaler environments to ensure that access is appropriate.	Inspected access review tickets for privileged users who have access to the Zscaler environments to determine that reviews are conducted on a monthly basis.	No exceptions noted.