



THALES DIS CPL CANADA, INC.

SOC 2 REPORT

FOR

DATA PROTECTION ON DEMAND SERVICES

A TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS
RELEVANT TO SECURITY, AVAILABILITY, CONFIDENTIALITY, AND PRIVACY

DECEMBER 1, 2023, TO NOVEMBER 30, 2024

Attestation and Compliance Services



Proprietary & Confidential

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

This report is intended solely for use by the management of Thales DIS CPL Canada, Inc., user entities of Thales DIS CPL Canada, Inc.'s services, and other parties who have sufficient knowledge and understanding of Thales DIS CPL Canada, Inc.'s services covered by this report (each referred to herein as a "specified user").

If the report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Schellman & Company, LLC as a result of such access. Further, Schellman & Company, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

TABLE OF CONTENTS

SECTION 1 INDEPENDENT SERVICE AUDITOR'S REPORT	1
SECTION 2 MANAGEMENT'S ASSERTION	5

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Thales DIS CPL Canada, Inc.:

Scope

We have examined Thales DIS CPL Canada, Inc.'s ("Thales" or the "service organization") accompanying description of its Data Protection on Demand Services ("DPoD Services") system, in Section 3, throughout the period December 1, 2023, to November 30, 2024, (the "description"), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria"), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period December 1, 2023, to November 30, 2024, to provide reasonable assurance that Thales' service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Thales uses various subservice organizations for data center hosting and cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Thales, to achieve Thales' service commitments and system requirements based on the applicable trust services criteria. The description presents Thales' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Thales' controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Thales is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Thales' service commitments and system requirements were achieved. Thales has provided the accompanying assertion, in Section 2, ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. Thales is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.

- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Service Auditor's Independence

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Test of Controls

The specific controls we tested, and the nature, timing, and results of those tests are presented in Section 4 of our report titled "Testing Matrices."

Opinion

In our opinion, in all material respects:

- the description presents Thales' DPoD Services system that was designed and implemented throughout the period December 1, 2023, to November 30, 2024, in accordance with the description criteria;
- the controls stated in the description were suitably designed throughout the period December 1, 2023, to November 30, 2024, to provide reasonable assurance that Thales' service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations applied the complementary controls assumed in the design of Thales' controls throughout that period; and
- the controls stated in the description operated effectively throughout the period December 1, 2023, to November 30, 2024, to provide reasonable assurance that Thales' service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Thales' controls operated effectively throughout that period.

Emphasis-of-Matter

Thales' description of its DPoD Services system states that incidents and breaches that involve personal information are investigated to identify the affected information, which is communicated to the data subjects, legal and

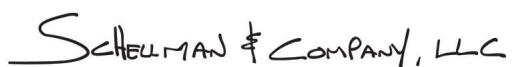
regulatory authorities, and others as required. However, during the period December 1, 2023, to November 30, 2024, no incidents or breaches occurred that would warrant the operation of the aforementioned controls. Because those controls did not operate during the period, we were unable to test, and did not test, the operating effectiveness of those controls as evaluated using trust services criteria “P6.3: The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity’s objectives related to privacy.”, “P6.5: The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident-response procedures to meet the entity’s objectives related to privacy.” and “P6.6: The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity’s objectives related to privacy.” Our opinion is not modified with respect to this matter.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Thales, user entities of Thales’ DPoD Services system during some or all of the period of December 1, 2023, to November 30, 2024, business partners of Thales subject to risks arising from interactions with the DPoD Services system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- the nature of the service provided by the service organization;
- how the service organization’s system interacts with user entities, business partners, subservice organizations, and other parties;
- internal control and its limitations;
- complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization’s service commitments and system requirements;
- user entity responsibilities and how they may affect the user entity’s ability to effectively use the service organization’s services;
- the applicable trust services criteria; and
- the risks that may threaten the achievement of the service organization’s service commitments and system requirements, and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

SCHEELMAN & COMPANY, LLC

Washington, District of Columbia
January 16, 2025

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of Thales' DPoD Services system, in Section 3, throughout the period December 1, 2023, to November 30, 2024, (the "description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria)*, ("description criteria"). The description is intended to provide report users with information about the DPoD Services system that may be useful when assessing the risks arising from interactions with Thales' system, particularly information about system controls that Thales has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and privacy ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Thales uses various subservice organizations for data center hosting and cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Thales, to achieve Thales' service commitments and system requirements based on the applicable trust services criteria. The description presents Thales' controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Thales' controls. The description does not disclose the actual controls at the subservice organizations.

We confirm, to the best of our knowledge and belief, that:

- the description presents Thales' DPoD Services system that was designed and implemented throughout the period December 1, 2023, to November 30, 2024, in accordance with the description criteria;
- the controls stated in the description were suitably designed throughout the period December 1, 2023, to November 30, 2024, to provide reasonable assurance that Thales' service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations applied the complementary controls assumed in the design of Thales' controls throughout that period; and
- the controls stated in the description operated effectively throughout the period December 1, 2023, to November 30, 2024, to provide reasonable assurance that Thales' service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Thales' controls operated effectively throughout that period.

Our description of our DPoD Services system states that incidents and breaches that involve personal information are investigated to identify the affected information, which is communicated to the data subjects, legal and regulatory authorities, and others as required. However, during the period December 1, 2023, to November 30, 2024, no incidents or breaches occurred that would warrant the operation of the aforementioned controls. Because those controls did not operate during the period, the tests of operating effectiveness could not be performed for those controls as evaluated using trust services criteria "P6.3: The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.", "P6.5: The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident-response procedures to meet the entity's objectives related to privacy.", and "P6.6: The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy."