REPORT ON INCOUNTRY, INC.'S DATA-RESIDENCY-AS-A-SERVICE PLATFORM RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY THROUGHOUT THE PERIOD DECEMBER 1, 2020 TO SEPTEMBER 30, 2021

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

COALFIRE CONTROLS

TABLE OF CONTENTS

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: InCountry, Inc. ("InCountry")

SCOPE

We have examined InCountry's accompanying assertion titled "Assertion of InCountry, Inc. Management" (assertion) that the controls within the Data-Residency-as-a-Service Platform (system) were effective throughout the period December 1, 2020 to September 30, 2021, to provide reasonable assurance that InCountry's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The description of the boundaries of the system indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at InCountry, to achieve InCountry's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the complementary user entity controls assumed in the design of InCountry's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

InCountry uses subservice organizations to provide data center colocation and cloud services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at InCountry, to achieve InCountry's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of InCountry's controls. 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

InCountry 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 InCountry's service commitments and system requirements were achieved. InCountry has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, InCountry is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

SERVICE AUDITOR'S RESPONSIBILITIES

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan

and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve InCountry's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve InCountry's service commitments and system requirements based on the applicable trust services criteria.

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

INHERENT LIMITATIONS

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 were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the 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.

OPINION

In our opinion, management's assertion that the controls within the Data-Residency-as-a-Service Platform were effective throughout the period December 1, 2020 to September 30, 2021, to provide reasonable assurance that InCountry's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of InCountry's controls operated effectively throughout that period is fairly stated, in all material respects.

Coalfire Controls LLC

Westminster, Colorado
December 16, 2021

SECTION 2

ASSERTION OF INCOUNTRY, INC. MANAGEMENT

4023 Kennett Pike #50376
Wilmington, DE 19807
USA
Incountry.com

Assertion of InCountry, Inc. (“InCountry”) Management

We are responsible for designing, implementing, operating and maintaining effective controls within the Data Residency-as-a-Service Platform (system) throughout the period December 1, 2020 to September 30, 2021, to provide reasonable assurance that InCountry’s service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

The description of the boundaries of the system indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at InCountry, to achieve InCountry’s service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the complementary user entity controls assumed in the design of InCountry’s controls.

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

We have performed an evaluation of the effectiveness of the controls within the system throughout the period December 1, 2020 to September 30, 2021, to provide reasonable assurance that InCountry’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) if complementary subservice organization controls and complementary user entity controls assumed in the design of InCountry’s controls operated effectively throughout that period. InCountry’s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period December 1, 2020 to September 30, 2021, to provide reasonable assurance that InCountry’s service commitments and system requirements were achieved based on the applicable trust services criteria.

InCountry, Inc.

ATTACHMENT A

INCOUNTRY, INC.'S DESCRIPTION OF THE BOUNDARIES OF ITS DATA-RESIDENCY-AS-A-SERVICE PLATFORM

TYPE OF SERVICES PROVIDED

InCountry, Inc. (“InCountry” or “the Company”) offers a Data Residency-as-a-Service Platform (“the Platform”), which focuses on data localization that securely stores and processes data in its country of origin. InCountry is headquartered in Wilmington, Delaware.

The system described in this section of the report details the InCountry Data Residency-as-a-Service Platform. Any other InCountry services are not included within the scope of this report. The accompanying description includes only the policies, procedures, and control activities at InCountry. It does not include the policies, procedures, and control activities at any subservice organizations (see below for a further discussion of subservice organizations).

The InCountry Data Residency-as-a-Service Platform provides the following in-scope services to customers.

INCOUNTRY SINGLE-TENANT

The InCountry single-tenant offering is a point of presence for customers, providing them with dedicated and secure hosts in every country. The customer operates with a dedicated infrastructure that is fully isolated from other network traffic. InCountry’s technical operations team fully manages all of the customer’s dedicated hosts across its points of presence, including system updates, system management, and backups.

Customers can continue to use the InCountry application programming interface (API), InCountry Software Development Kit (SDK), InCountry Border, or InCountry Salesforce integration package with their single-tenant hosts, with the option to integrate additional countries with shared infrastructure.

INCOUNTRY MULTI-TENANT

The InCountry multi-tenant offering is a point of presence for customers, providing them with a secure multi-tenant version of the InCountry platform. The Platform is based on multi-tenant provisioning and operates as a managed service. Similar to the single-tenant offering, InCountry’s technical operations team will fully manage all of the customer’s provisioned assets across its points of presence, including system updates, system management, and backups.

INCOUNTRY REST API AND INCOUNTRY SDK

The InCountry point of presence API is a RESTful API and provides a customer with secure endpoints to store and manage their data within InCountry’s environment. It is a basis for the functionality of the InCountry SDK. The InCountry SDK is an easily embedded set of tools that performs client-side encryption and decryption of customer data and manages storage across InCountry’s worldwide points of presence. The InCountry SDK is available in Java, Node.js, Python, and C# and uses each language’s underlying encryption libraries. The customer retains the encryption keys.

The InCountry SDK can connect directly to any point of presence in InCountry’s network or be transmitted via the nearest point of presence in a customer’s target country to accelerate connectivity worldwide.

INCOUNTRY BORDER

InCountry Border enables personal information to be fully contained within the country of origin. Web service calls between a customer’s users’ web browsers and a globally distributed web application are passed through InCountry’s points of presence in specified countries. Personal information is automatically

removed, stored, and encrypted within InCountry's systems based on the predefined rules. This data can also be decrypted and reinserted via web service calls.

InCountry Border is deployed by a customer's operations team with no coding changes to the customer's application. Seamless security is provided with a domain overlay model so that web service calls and authentication cookies can be passed to a customer's existing web service endpoints.

INCOUNTRY DATA RESIDENCY FOR SALESFORCE

The InCountry Salesforce application package is an external component developed and maintained by InCountry. This component allows customers to securely operate with InCountry SDK and InCountry Border within their Salesforce instance. It includes all features available for regular InCountry SDK and InCountry Border users, allowing them to operate with the necessary data only within the borders of their country of origin.

INCOUNTRY PAYMENT GATEWAY

InCountry Payment Gateway enables cardholder data (CHD) to be fully stored within its country of origin and securely transmitted to globally distributed payment service providers on demand.

Web service calls between a customer's users' web browsers and the customer's backend are passed through InCountry's points of presence in specified countries. CHD is automatically encrypted and stored within InCountry's points of presence, providing the customer's backend with redacted data.

Upon authorized request from the customer's backend, CHD is unredacted and transmitted to a payment service provider for further processing.

THE BOUNDARIES OF THE SYSTEM USED TO PROVIDE THE SERVICES

The boundaries of the InCountry Data Residency-as-a-Service Platform are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the InCountry Data Residency-as-a-Service Platform.

The components that directly support the services provided to customers are described in the subsections below.

INFRASTRUCTURE

InCountry utilizes Amazon Web Services (AWS), Alibaba Cloud, Microsoft Azure, Google Cloud Platform (GCP), Oracle Cloud Infrastructure (OCI), Yandex.Cloud, TeamCloud Solution (TheGigabit), OneProvider, Web.com.ph, CloudSigma Research Ltd., IsNet, and Selectel Cloud Platform (hereafter, InCountry's Subcontracted Hosting Services) to provide the resources to host the InCountry Data Residency-as-a-Service Platform. The Company is responsible for designing and configuring the InCountry data residency-as-a-service architecture within InCountry's Subcontracted Hosting Services to ensure the availability, security, and resiliency requirements are met.

A limited group of authorized users access the production environment via a bastion host. These users are authenticated via password and multi-factor authentication (MFA) tokens. Once in the environment, these users must authenticate on the individual hosts to which they require access.

InCountry uses PostgreSQL for its primary database systems. All databases are hosted in the environments of InCountry's Subcontracted Hosting Services. Customer databases are logically segmented from one another.

The in-scope hosted infrastructure consists of supporting tools as shown in the table below:

Infrastructure	
Production Tool	**Business Function**
Bastion	Administration
PostgreSQL	Customer data storage

SOFTWARE

Software consists of the programs and software that support the InCountry Data Residency-as-a-Service Platform (operating systems [OSs], middleware, and utilities). The list of software and ancillary software used to build, support, secure, maintain, and monitor the InCountry Data Residency-as-a-Service Platform include the following applications, as shown in the table below:

Software	
Production Application	**Business Function**
Zabbix	Application and infrastructure monitoring
pg_probackup	Backup and replication
Threat Stack	Security incident and event management (SIEM) and logging, file integrity monitoring (FIM), intrusion detection
ClamAV	Antivirus
Jira	Help desk and ticketing system
GitHub	Web-based platform used for version control
Microsoft Intune	Mobile device management system
Splunk	SIEM tool
Nebula	Overlay networking tool
Travis CI	Unified solution for building all Docker images for all app and service repositories
Jenkins	CI/CD server for automated builds, deploys, tests, etc.
Zephyr	Test management tool

Software	
Production Application	**Business Function**
Opsgenie	Alerting and incident response tool
JumpCloud	Corporate single sign-on (SSO)
Grafana	Analytics and monitoring solution
Elasticsearch	A distributed search and analytics engine
Snyk	Code review tool (static application security testing [SAST])
SonarSource (SonarCloud)	Code analyzer (SAST)
Burp Suite Professional	Application security testing solution (dynamic application testing solution [DAST])
Sentry.io	Error tracking tool
Tenable.io	Vulnerability management tool
HashiCorp Vault	Secret management tool

PEOPLE

The Company develops, manages, and secures the InCountry Data Residency-as-a-Service Platform via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Executive Management	Responsible for overseeing Company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
Engineering	Responsible for the development, testing, and maintenance of the software for the InCountry Data Residency-as-a-Service Platform.
Operations	Responsible for operation of the service, including the implementation of access controls, configuration management, deployment of new builds and features, monitoring of the performance and availability of the service, and incident response.
Trust and Security	Responsible for application and infrastructure security, access control management, privacy, compliance, vendor management, internal controls monitoring, security incident response, corporate IT functions, and risk management.
Human Resources (HR)	Responsible for onboarding new personnel, defining the roles and positions of new hires, performing background checks, and facilitating the employee termination process.

PROCEDURES

Procedures include the automated and manual procedures involved in the operation of the InCountry Data Residency-as-a-Service Platform. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, information technology (IT), and HR. These procedures are drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business, but no less than annually.

The following table details the procedures as they relate to the operation of the InCountry Data Residency-as-a-Service Platform:

Procedures	
Procedure	**Description**
Logical Access	How the Company restricts logical access, provides, and removes that access, and prevents unauthorized access.
Software Development Life Cycle (SDLC)	How the Company develops code following secure development principles.
Security Incident Response	How the Company reacts to information security incidents.
Operations Management	How the Company manages the operation of the system and detects and mitigates processing deviations, including logical and physical security deviations.
Change Management	How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk Management	How the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

DATA

Data refers to transaction streams, files, data stores, tables, and output used or processed by InCountry. Via the Platform, customers or end users define and control the data they load and store in the Platform's production network. This data is loaded into the environment and accessed remotely from customer systems via the Internet.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts.

The Company has deployed secure methods and protocols for the transmission of confidential or sensitive information over public networks.

The following table details the types of data contained in the production application for the InCountry Data Residency-as-a-Service Platform:

Data	
Production Application	**Description**
Usage information	InCountry keeps track of user activity in relation to the types of services customers and their users use, the configuration of their computers, and performance metrics related to their use of the services.
User and account data	This includes PII, protected health information (PHI), and other data from InCountry's employees, customers, users (customers' employees), and other third parties, such as suppliers, vendors, business partners, and contractors. This collection is permitted under the Terms of Service and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Access to PII and PHI is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job function.
Log information	InCountry logs information about customers and their users, including Internet Protocol (IP) addresses. Log files are immutable records of computer events about an OS, application, or user activity, which form an audit trail. These records may be used to assist in detecting security violations, performance problems, and flaws in applications.
Metadata	Metadata consists primarily of tags, which are typically formatted in key: value (e.g., env: prod) format. Metadata enables data such as infrastructure metrics, application performance management (APM), and logs to be filtered and grouped. Metadata does not contain personal data as part of the intended use of the service.

COMPLEMENTARY USER ENTITY CONTROLS (CUECS)

The Company's controls related to the InCountry Data Residency-as-a-Service Platform cover only a portion of overall internal control for each user entity of the InCountry Data Residency-as-a-Service Platform. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by the Company. Therefore, each user entity's internal control should be evaluated in conjunction with the Company's controls, taking into account the related CUECs identified for the specific criterion. Each user entity must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

The CUECs presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. Management of user entities is responsible for the following:

Criteria	Complementary User Entity Controls
CC2.1	• User entities have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by the Company according to contractually specified time frames. • Controls to provide reasonable assurance that the Company is notified of changes in: – User entity vendor security requirements – The authorized users list
CC2.3	• It is the responsibility of the user entity to have policies and procedures to: – Inform their employees and users that their information or data is being used and stored by the Company. – Determine how to file inquiries, complaints, and disputes to be passed on to the Company.
CC6.1	• User entities grant access to the Company's system to authorized and trained personnel. • User entities utilize InCountry SDK to encrypt their data prior to InCountry receiving the data. • User entities restrict access to encryption keys to appropriate personnel. • Controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by the Company.
CC6.4 CC6.5 CC7.2 A1.2	• User entities deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity.

SUBSERVICE ORGANIZATIONS AND COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCS)

The Company uses AWS, Alibaba Cloud, Microsoft Azure, GCP, OCI, Yandex.Cloud, TeamCloud Solution (TheGigabit), OneProvider, Web.com.ph, CloudSigma Research Ltd., IsNet, and Selectel Cloud Platform as subservice organizations for data center colocation and cloud services. InCountry's controls related to the Data Residency-as-a-Service Platform cover only a portion of the overall internal control for each user entity of the InCountry Data Residency-as-a-Service Platform.

Although the subservice organizations have been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organizations. CSOCs are expected to be in place in data center provider environments related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. Physical security controls mitigate the risk of fires, power loss, climate, and temperature variabilities.

Company management annually receives and reviews the SOC 2 reports of InCountry's Subcontracted Hosting Services. In addition, through its operational activities, InCountry management monitors the services performed by the data center providers to determine whether operations and controls expected to be implemented at the subservice organizations are functioning effectively. Management also has communication with the subservice organizations to monitor compliance with the service agreements, stay abreast of changes planned at hosting facilities, and relay any issues or concerns to subservice organization management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to the InCountry Data Residency-as-a-Service Platform to be achieved solely by InCountry. Therefore, each user entity's internal control must be evaluated in conjunction with InCountry's controls, taking into account the related CSOCs expected to be implemented at the subservice organizations as described below.

Criteria	Complementary Subservice Organization Controls
CC6.1	• Data center providers are responsible for encrypting data stores at rest.
CC6.4	• Data center providers are responsible for restricting data center access to authorized personnel. • Data center providers are responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC6.5 CC6.7 C1.2	• Data center providers are responsible for securely decommissioning and physically destroying production assets in its control.
CC7.2 A1.2	• Data center providers are responsible for the installation of fire suppression and detection and environmental monitoring systems at the data centers. • Data center providers are responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • Data center providers are responsible for overseeing the regular maintenance of environmental protections at data centers.

SIGNIFICANT CHANGES TO THE SYSTEM

In August 2021, additional data center locations hosted by GCP and IsNet were deployed for customer use. Additionally, Equinix was decommissioned as a data center vendor in April 2021. There were no other changes that are likely to affect report users' understanding of how the InCountry Data Residency-as-a-Service Platform is used to provide the service from December 1, 2020 to September 30, 2021.

ATTACHMENT B

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Commitments are declarations made by management to customers regarding the performance of the InCountry Data Residency-as-a-Service Platform. Commitments are communicated within the InCountry Master Service agreement, Terms of Use, Data Processing Addendum, and the Privacy Policy.

System requirements are specifications regarding how the InCountry Data Residency-as-a-Service Platform should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures.

The Company's principal service commitments and system requirements related to the InCountry Data Residency-as-a-Service Platform include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• Protect personal identifying information (PII) and the security of the information system from unauthorized access, use, modification, disclosure, destruction, threats, or hazards. • Develop, implement, and maintain an information security program designed to protect the security, integrity, and confidentiality of the system and its information.	• Information security policy • Security incident response plan • Physical and environmental security standards • Vulnerability management standards • Third-party management standards • Security incident response plan • Change management standards • Risk management standards
Availability	• InCountry endeavors to have 99.9% monthly uptime percentage.	• Business continuity management (BCM) standards • Physical and environmental security standards
Confidentiality	• Maintain all customer data as confidential, and do not disclose information to any unauthorized parties without written consent. • InCountry shall use at least the same degree of care it uses to prevent the disclosure of its own confidential information, to prevent the disclosure of customer data.	• Asset classification and protection management standards • Deletion and retention policy

Trust Services Category	Service Commitments	System Requirements
	• Upon expiration or termination of the agreement for any reason, InCountry shall deliver to the customer all of the customer's confidential information that InCountry may have in its possession or control or, at the customer's option, shall destroy all confidential information and certify the destruction in writing once the agreement has been terminated. • InCountry shall ensure that its personnel engaged in the processing of personal data are informed of the confidential nature of the personal data, have received appropriate training on their responsibilities and have executed written confidentiality agreements. • InCountry will not: (a) use any confidential information of the disclosing party for any purpose other than to exercise its rights or to perform its obligations under the master service agreement; or (b) disclose, publish, or disseminate confidential information of the disclosing party to anyone other than the receiving party's employees who have a need to know.	