REPORT ON INCOUNTRY, INC.'S DATA-RESIDENCY-AS-A-SERVICE PLATFORM RELEVANT TO SECURITY, AVAILABILITY AND CONFIDENTIALITY THROUGHOUT THE PERIOD OCTOBER 1, 2019 TO DECEMBER 31, 2019

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

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 InCountry's Data-Residency-as-a-Service Platform (system) were effective throughout the period October 1, 2019 to December 31, 2019, 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*).

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 InCountry'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 InCountry'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 InCountry'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 InCountry's Data-Residency-as-a-Service Platform were effective throughout the period October 1, 2019 to December 31, 2019, to provide reasonable assurance that InCountry's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Restricted Use

Certain 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. Users of this report should have sufficient knowledge and understanding of 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. InCountry uses Amazon Web Services (AWS), Alibaba, NTT, Equinix, and AT&T/Evoque as a data center colocation providers. Users of this report should obtain the relevant AWS, Alibaba, NTT, Equinix, and AT&T/Evoque SOC 2 or SOC 3 reports.

Coalfire Controls LLC

Westminster, Colorado
January 2, 2020

SECTION 2

ASSERTION OF INCOUNTRY, INC. MANAGEMENT

InCountry, Inc.
228 Grant Avenue, Suite 5
San Francisco, CA. 94108
Phone 425.677.5308
info@incountry.com
www.incountry.com

Assertion of InCountry, Inc. Management ("InCountry")

We are responsible for designing, implementing, operating and maintaining effective controls within InCountry's Data-Residency-as-a-Service Platform (system) throughout the period October 1, 2019 to December 31, 2019 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.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 1, 2019 to December 31, 2019, 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*). 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 October 1, 2019 to December 31, 2019, 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 the 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 San Francisco, CA, with operations in Minsk, Belarus. The InCountry Data-Residency-as-a-Service Platform provides the following in-scope services to customers:

INCOUNTRY SOFTWARE DEVELOPMENT KIT (SDK)

The InCountry SDK performs client-side encryption and decryption of customer data and manages storage across InCountry’s worldwide points of presence. The SDK is available in Java, Node, and Python, and uses each platform’s underlying encryption libraries. The customer retains the encryption keys.

The 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 server’s country to accelerate connectivity worldwide.

INCOUNTRY BORDER

InCountry Border enables personal information to be fully contained within a country’s borders. Web service calls between a customer’s users’ web browsers and a customer’s globally-distributed web application is proxied through InCountry’s points of presence in specified countries. Personal information is automatically removed and stored, encrypted, within InCountry’s systems. This data can also be decrypted and reinserted via web service calls.

InCountry Border can be 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 MANAGED SERVICE PROVIDER (MSP)

InCountry’s MSP offering provides customers with dedicated and secure hosts in every country in which the customer operates with dedicated infrastructure that is fully isolated from other network traffic. InCountry’s network operations team will fully manage a customer’s dedicated hosts across all its points of presence, including system updates, system management, and backups.

Customers can continue to use InCountry SDK or InCountry Border in their own dedicated hosts, with the option to interleave additional countries with shared infrastructure.

THE COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

The boundaries of the system 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 system.

The components that directly support the services provided to customers are described in the sub-sections below.

INFRASTRUCTURE

The Company utilizes Amazon Web Services (AWS), Alibaba, NTT, Equinix, and AT&T/Evoque 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 AWS, Alibaba, NTT, Equinix, and AT&T/Evoque to ensure that the availability, security, and resiliency requirements are met.

A limited group of authorized users access the production environment via a bastion host over a Secure Shell (SSH) connection. These users are authenticated via password-protected SSH certificates. Once in the environment, these users must authenticate on the individual hosts to which they require access. InCountry uses Postgres for its primary database systems. All databases are hosted in InCountry's AWS, Alibaba, NTT, Equinix, and AT&T/Evoque cloud environments. Customer databases are logically segmented from one another.

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

INFRASTRUCTURE			
Production Tool	**Business Function**	**Operating System**	**Hosted Location**
Databases	Customer data storage	Postgres	AWS, Alibaba, NTT, Equinix, and AT&T/Evoque

SOFTWARE

Software consists of the application programs and information technology (IT) system software that supports application programs (operating systems, 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:

SOFTWARE	
Production Application	**Business Function**
Postgres	Database that stores customer data
Zabbix	Application and infrastructure monitoring
WAL-G	Backup and replication
Threat Stack	Security incident and event management (SIEM) and logging system, file integrity monitoring (FIM), intrusion detection and prevention
ClamAV	Antivirus
Jira	Helpdesk and ticketing system
Intune	Mobile device management system

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 new code for the InCountry Data-Residency-as-a-Service Platform.
Operations	Responsible for operation of the service, including the management of access control, deployment of new builds and features, monitoring of performance and availability of the service, and incident response.
Trust and Security	Responsible for application and infrastructure security, privacy, compliance, vendor management, internal control 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 engineering, operations, security, 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.

PROCEDURES	
Procedure	**Description**
Logical Access	How the Company restricts logical access, provides and removes that access, and prevents unauthorized access.
Software Development Lifecycle (SDLC)	How the Company develops code following secure development principles as well as controls and reviews.
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.

PROCEDURES	
Procedure	**Description**
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 Mitigation	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. Customers or end-users define and control the data they load and store in the InCountry Data-Residency-as-a-Service Platform production network via the Platform. 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. All the data sent by the customer should be encrypted.

DATA		
Production Application	**Description**	**Data Store**
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.	Relational Database Service (RDS) databases, Elasticsearch
User and account data	Personally Identifiable Information (PII), Protected Health Information (PHI), and other data from its employees, customers, users (customers' employees), and other third parties such as suppliers, vendors, business partners, and contractors.	RDS databases
Log information	InCountry logs information about customers and their users, including Internet Protocol (IP) address. Log files are immutable records of computer events about an operating system, 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.	SIEM tool, Elasticsearch, RDS

DATA		
Production Application	**Description**	**Data Store**
Metadata	Metadata consists primarily of tags, which are typically formatted in the key:value (e.g., env:prod) format. Metadata enables customer data such as infrastructure metrics, application performance management (APM), and logs to be filtered and grouped. Metadata should not contain personal data as part of the intended use of the service.	Consul

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 Terms of Service agreement 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, which are available to all employees.

The Company's principal service commitments and system requirements include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• Protect personal identifying information 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	• None	• Business continuity management standards • Physical and environmental security standards

Trust Services Category	Service Commitments	System Requirements
Confidentiality	• Maintain all customer data as confidential and do not disclose information to any unauthorized parties without written consent. • Use at least the same degree of care it uses to prevent the disclosure of InCountry's own confidential information. • Upon expiration or termination of the agreement for any reason, InCountry shall deliver to Customer all of the Customer's confidential information that InCountry may have in its possession or control or, at Customer's option, shall destroy all confidential information and certify the destruction in writing once the agreement has been terminated.	• Asset classification and protection management standards • Deletion and retention policy