



**TECH5 USA, INC.**

**Independent Service Auditor's Report SOC 3® at a Service  
Organization Relevant to Security**

**November 1, 2024, through January 31, 2025**

**[www.AARC-360.com](http://www.AARC-360.com)**

## Table of Contents

<b>SECTION 1 – INDEPENDENT SERVICE AUDITOR’S REPORT .....</b>	<b>2</b>
<b>SECTION 2 – ASSERTION OF TECH5 USA, INC. MANAGEMENT.....</b>	<b>5</b>
<b>SECTION 3 – TECH5 USA, INC.’S DESCRIPTION OF ITS LAW ENFORCEMENT 2.0 (LE2) SYSTEM .....</b>	<b>7</b>
TECH5 USA OVERVIEW .....	8
PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS.....	8
COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES .....	9
INFRASTRUCTURE .....	9
SOFTWARE .....	9
PEOPLE.....	10
<b>SECTION 4 – TECH5 USA, INC.’S PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS .....</b>	<b>11</b>
PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS.....	12
COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCs) .....	13
COMPLEMENTARY USER ENTITY CONTROLS.....	14

---

## **SECTION 1 – INDEPENDENT SERVICE AUDITOR’S REPORT**

---

## Independent Service Auditor's Report

**To: TECH5 USA, INC.**

### *Scope*

We have examined TECH5 USA, Inc.'s ('TECH5 USA', 'the Company', or 'the Service Organization') accompanying assertion titled "Assertion of TECH5 USA, Inc. Management" (assertion) that the controls within TECH5 USA's Law Enforcement 2.0 (LE2) (system) were effective throughout the period November 1, 2024, through January 31, 2025, to provide reasonable assurance that TECH5 USA's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (with Revised Points of Focus – 2022)* in AICPA Trust Services Criteria.

TECH5 USA uses Amazon Web Services (AWS' or 'the Subservice Organization') to provide Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at TECH5 USA, to achieve TECH5 USA's service commitments and system requirements based on the applicable trust services criteria. The description presents TECH5 USA's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of TECH5 USA's controls. The description does not disclose the actual controls at the Subservice Organization. Our examination did not include the services provided by the Subservice Organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at TECH5 USA, to achieve TECH5 USA's service commitments and system requirements based on the applicable trust services criteria. The description presents TECH5 USA's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of TECH5 USA'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.

### *Service Organization's Responsibilities*

TECH5 USA 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 TECH5 USA's service commitments and system requirements were achieved. TECH5 USA has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, TECH5 USA is responsible for selecting, and identifying in its assertion, the applicable trust services 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 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 AICPA. 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.

---

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

Our examination included the following:

- 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 TECH5 USA'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 TECH5 USA's service commitments and system requirements based 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 TECH5 USA's Law Enforcement 2.0 (LE2) were effective throughout the period November 1, 2024, through January 31, 2025, to provide reasonable assurance that TECH5 USA's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

# AARC-360

Alpharetta, Georgia  
March 3, 2025

## **SECTION 2 – ASSERTION OF TECH5 USA, INC. MANAGEMENT**

## Assertion of TECH5 USA, INC. Management

March 3, 2025

We are responsible for designing, implementing, operating, and maintaining effective controls within TECH5 USA, Inc.'s ('TECH5 USA', 'the Company', or 'the Service Organization') Law Enforcement 2.0 (LE2) (system) November 1, 2024, through January 31, 2025, to provide reasonable assurance that TECH5 USA's service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (with Revised Points of Focus – 2022)* in AICPA Trust Services Criteria. Our description of the boundaries of the system is presented Section 3 and identifies the aspects of the system covered by our assertion.

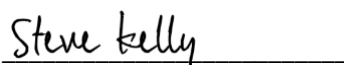
TECH5 USA uses Amazon Web Services (AWS' or 'the Subservice Organization') to provide Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at TECH5 USA, to achieve TECH5 USA's service commitments and system requirements based on the applicable trust services criteria. The description presents TECH5 USA's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of TECH5 USA's controls. The description does not disclose the actual controls at the Subservice Organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at TECH5 USA, to achieve TECH5 USA's service commitments and system requirements based on the applicable trust services criteria. The description presents TECH5 USA's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of TECH5 USA's controls.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period November 1, 2024, through January 31, 2025, to provide reasonable assurance that TECH5 USA's service commitments and system requirements were achieved based on the applicable trust services criteria. TECH5 USA'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 Section 4.

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 November 1, 2024, through January 31, 2025, to provide reasonable assurance that TECH5 USA's service commitments and system requirements were achieved based on the applicable trust services criteria.

A handwritten signature in black ink that reads "Steve Kelly".

Steve Kelly  
Managing Director  
TECH5 USA, Inc.

**SECTION 3 – TECH5 USA, INC.’S DESCRIPTION OF ITS LAW ENFORCEMENT 2.0  
(LE2) SYSTEM**



## **TECH5 USA, INC.'s Description of Its Law Enforcement 2.0 (LE2) throughout the period November 1, 2024, through January 31, 2025**

### **TECH5 USA Overview**

TECH5 USA, Inc. ('TECH5 USA', the Service Organization', or 'the Company') is a provider of a worldwide cloud-based biometric software application. The Company processes customer requests via an application programming interface (API). The Law Enforcement 2.0 (LE2) System ("the System") provides TECH5 USA customers ("customers") and their clients with an end-to-end solution that harnesses the power of advanced biometric technology to enhance community safety for law enforcement and government agencies to offer the highest accuracy and speed in identity verification, improving investigative and operational efficiency ("the services").

### **Scope of This Report**

This report is intended to provide thorough descriptions of the controls of the System provided by the Company for its customers. This description details the LE2 System and the related policies, procedures, and control activities for the System which are in-scope for this report. The related locations included in scope are resources and offerings located within the United States of America.

This description does not include any other TECH5 USA services not referenced above and does not include the policies, procedures, and control activities at the Subservice Organization (see below for further discussion of the Subservice Organization).

### **Principal Service Commitments and System Requirements**

TECH5 USA designs its processes and procedures related to the System to meet its objectives for its services. Those objectives are based on the service commitments that TECH5 USA makes to its customers, business partners, vendors, and the Subservice Organization and the operational and compliance requirements that TECH5 USA has established for the services. Service commitments are declarations made by management to its customers regarding the performance of the System. Service commitments are set forth in standard contracts, service level agreements, and in the description of the service offering provided online and include the following:

- Commitments regarding the security of the System and of information processed by the System in accordance with contractual stipulations.
- Commitments to support customer compliance with the security-related requirements set forth in services agreements.

TECH5 USA establishes operational requirements that support the achievement of security commitments, relevant operational and compliance requirements, applicable laws and regulations, and other system requirements including the following:

- System functional and nonfunctional requirements derived from service commitments, published documentation of System functionality, and other descriptions of the System.
- Monitoring of third-party providers to detect failures of those service providers to meet service agreements that could threaten the achievement of the Company's service commitments and System requirements and respond to those failures. Such requirements are communicated in TECH5 USA system policies and procedures, system design documentation, and contracts with customers.

TECH5 USA has adopted a cybersecurity framework as the basis for its organization-wide information security policies. In addition to these policies, standard operating procedures have been developed and documented on how to carry out specific manual and automated processes required in the operation and development of the System. System requirements based on the selected cybersecurity framework include the following:

- Data, personnel, devices, systems, and facilities are identified and managed.
- TECH5 USA management identifies, assesses, and manages cybersecurity risk to organizational operations.

- TECH5 USA priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
- Access to logical assets is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
- Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
- Security policies, processes, and procedures are maintained and used to manage protection of information systems and assets.
- Technical security solutions are managed to help ensure the security and resilience of systems and assets.
- Anomalous activity is detected, and the potential impact of events is understood.
- The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
- Detection processes and procedures are maintained and tested to help ensure awareness of anomalous events.
- Response processes and procedures are executed and maintained to help ensure response to detected cybersecurity incidents.
- Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.

## Components of the System Used to Provide the Services

The System described herein is bound by the specific aspects of TECH5 USA's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers and the data that is processed by the System. 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 user entities are as follows:

### Infrastructure

Each TECH5 USA customer's LE2 instance is hosted on infrastructure that is exclusive to the customer. The infrastructure includes a production and testing environment. Each environment exists in its own AWS account.

TECH5 USA utilizes Amazon Web Services (AWS) as a subservice organization to host the System. TECH5 USA leverages the experience and resources of AWS to enable TECH5 USA to achieve its service commitments and system requirements. AWS is responsible for designing and configuring the System architecture within AWS to help ensure service commitments and system requirements are met. TECH5 USA's System utilizes the AWS GovCloud service support of security commitments. The policies, procedures and control activities of AWS are carved-out of this report (see below for further discussion of the Subservice Organization).

### Software

The software component consists of the applications, programs, and other software that support the System. The list of software and ancillary software used to build, support, secure, maintain, and monitor the System are the following:

Production Applications	Business Function
TECH5 USA LE2	TECH5 USA 's public safety solutions harness the power of advanced biometric technology to enhance community safety for law enforcement and government agencies. With FBI-certified technologies, our solutions offer the highest accuracy and speed in identity verification, improving investigative and operational efficiency.

Various tools are in place to support the applications in-scope as noted above and assist in the processing of IT general controls. Significant tools in-scope for this report include:

Production Software	Business Function
Jira	Tool utilized for Incident Management documentation, review, and resolution. Also utilized for Change Management documentation, including testing and approval details.
GitHub	Tool utilized for source code management and software building.
Salesforce	Tool utilized for Customer Support tracking.
PagerDuty	Tool for alerting.

## People

TECH5 USA has various personnel groups that directly support the System. The responsibilities of these groups are defined in the following table:

Group/Role Name	Business Function
Executive Management	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives.
Engineering	Responsible for the development, testing, deployment, and maintenance of new code for the System.
Product Management	Responsible for the LE2 product life cycle, including adding additional product functionality.
Human Resources and Accounting	Responsible for onboarding new personnel, defining the role/ position of new hires, performing background checks, and facilitating the employee termination/offboarding process. Staff that provide the day-to-day services such as invoicing, payment processing, payment tracking, reconciliation, and mitigation of past due payments.
Operations	Operations includes the support team responsible for resolving issues raised by users of the System, security and compliance, vendor management, Information Technology and Program Management.
IT	Information Technology (IT) is responsible for maintaining ancillary, non-production systems to support TECH5 USA personnel.
DevOps	Responsible for operating, maintaining and monitoring the infrastructure services provided by the Subservice Organization.

## Procedures

TECH5 USA has developed and communicated policies and procedures involved in the operation of the System. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to risk management, data backup, system access, auditing, configuration management, breach/incidents, disaster recovery, intrusion detection, vulnerability assessment, data integrity, vendor management, and so on. These procedures are developed in alignment with the overall information security policy and are reviewed, updated, and approved as necessary for changes in the business, but no less than once annually.

## **SECTION 4 – TECH5 USA, INC.’S PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS**

## Principal Service Commitments and System Requirements

TECH5 USA designs its processes and procedures related to the System to meet its objectives for its services. Those objectives are based on the service commitments that TECH5 USA makes to its customers, business partners, vendors, and the Subservice Organization and the operational and compliance requirements that TECH5 USA has established for the services. Service commitments are declarations made by management to its customers regarding the performance of the System. Service commitments are set forth in standard contracts, service level agreements, and in the description of the service offering provided online and include the following:

- Commitments regarding the security of the System and of information processed by the System in accordance with contractual stipulations.
- Commitments to support customer compliance with the security-related requirements set forth in services agreements.

TECH5 USA establishes operational requirements that support the achievement of security commitments, relevant operational and compliance requirements, applicable laws and regulations, and other system requirements including the following:

- System functional and nonfunctional requirements derived from service commitments, published documentation of System functionality, and other descriptions of the System.
- Monitoring of third-party providers to detect failures of those service providers to meet service agreements that could threaten the achievement of the Company's service commitments and System requirements and respond to those failures. Such requirements are communicated in TECH5 USA system policies and procedures, system design documentation, and contracts with customers.

TECH5 USA has adopted a cybersecurity framework as the basis for its organization-wide information security policies. In addition to these policies, standard operating procedures have been developed and documented on how to carry out specific manual and automated processes required in the operation and development of the System. System requirements based on the selected cybersecurity framework include the following:

- Data, personnel, devices, systems, and facilities are identified and managed.
- TECH5 USA management identifies, assesses, and manages cybersecurity risk to organizational operations.
- TECH5 USA priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
- Access to logical assets is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
- Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
- Security policies, processes, and procedures are maintained and used to manage protection of information systems and assets.
- Technical security solutions are managed to help ensure the security and resilience of systems and assets.
- Anomalous activity is detected, and the potential impact of events is understood.
- The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
- Detection processes and procedures are maintained and tested to help ensure awareness of anomalous events.
- Response processes and procedures are executed and maintained to help ensure response to detected cybersecurity incidents.
- Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.

## Complementary Subservice Organization Controls (CSOCs)

The description does not extend to the services provided by Amazon Web Services (AWS' or 'the Subservice Organization'). Section 4 of this report and the description of the System only cover the relevant trust services criteria and related controls in support of the achievement of TECH5 USA's service commitments and system requirements and exclude the related controls of the Subservice Organization.

Although the Subservice Organization has been carved out for the purposes of this report, TECH5 USA management has assumed, in the design of the System, that certain complementary subservice organization controls (CSOCs) would be implemented by the Subservice Organization. Such controls are necessary, in combination with controls at TECH5 USA, to provide reasonable assurance that TECH5 USA's service commitments and system requirements were achieved. Because the related service commitments and system requirements can only be achieved if the CSOCs are suitably designed and operating effectively during the period November 1, 2024 through January 31, 2025, each user entity must evaluate TECH5' USA s controls, related tests of controls, and results of tests described in section 4 of this report, considering the types of related CSOCs expected to be implemented at the Subservice Organization as shown below.

Subservice Organization	Services Provided	Expected CSOCs
AWS	Infrastructure	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of an employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Closed circuit television cameras (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
		Access to server locations is managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
		Data centers are protected by fire detection and suppression systems.
		Data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels
		Data centers are monitored for power outages and have generators to provide backup power in case of electrical failure.
		Changes to customer-affecting aspects of a service are reviewed, tested, and approved.
		Separate production and development environments are maintained.
		Changes are reviewed for business impact and approved by authorized personnel prior to migration to production.

Subservice Organization	Services Provided	Expected CSOCs
		Deployment validations and change reviews are performed to detect unauthorized changes to the environment.
		Production media is securely decommissioned, physically destroyed, and verified prior to leaving the data center.

The management of TECH5 USA performs vendor risk reviews on an annual basis for each of its vendors, including the Subservice Organization. The vendor risk reviews can include the evaluation independent third-party assessment reports of its vendors. In addition, management monitors the services performed by the Subservice Organization to determine whether operations and controls expected to be implemented at the Subservice Organization are suitably designed and operating effectively. In addition, TECH5 USA management monitors the services performed by the Subservice Organization to determine whether operations and controls expected to be implemented at the Subservice Organization are suitably designed and operating effectively.

Management monitors the Subservice Organization status page to stay informed of any changes in the services performed and has a customer support portal to relay any issues or concerns to the Subservice Organization's management.

### Complementary User Entity Controls

Certain criteria specified in the description can be achieved only if complementary user entity controls contemplated in the design of TECH5 USA's controls are suitably designed and operating effectively, along with related controls at TECH5 USA. Complementary User Entity Controls are specific user controls or issues each TECH5 USA client organization should implement or address respectively in order to achieve the applicable criteria identified in this report. These considerations are not necessarily a comprehensive list of all internal controls that should be employed by user entities, nor do they represent procedures that may be necessary in all circumstances.

Complementary User Entity Controls
User entities have policies and procedures that require reporting any material changes to their control environment that may adversely affect the ability of TECH5 USA to deliver service. User entities have controls that require providing notice to TECH5 USA of any material changes in security requirements and the authorized users list.
User entities have policies and procedures to determine how to file inquiries, complaints, or disputes to TECH5 USA.
User entities are responsible for having a process in place to provision TECH5 USA support users to their environment.
User entities deploy physical security and environmental controls for local and remote devices and access points that access the TECH5 USA System.
User entities have policies and procedures for controlling user IDs and passwords that are used to access the TECH5 USA System.