Insight Assurance

SOC 2 | ISO 27001 | PCI | HIPAA

System and Organization Controls (SOC) 3
Report on QuesTek Innovations LLC's ICMD® Services System
Relevant to Security For the Period
November 27, 2023, to February 26, 2024

QUESTEK® INNOVATIONS LLC

TABLE OF CONTENTS

INDEPENDENT SERVICE AUDITOR'S REPORT

Insight Assurance
SOC 2 | ISO 27001 | PCI | HIPAA

INDEPENDENT SERVICE AUDITOR'S REPORT ON A SOC 3 EXAMINATION

To: QuesTek Innovations LLC

Scope

We have examined QuesTek Innovations LLC's ('QuesTek Innovations) accompanying assertion titled " QuesTek Innovations LLC's Management Assertion" (assertion) that the controls within QuesTek Innovations' ICMD® Services System (system) were effective throughout the period November 27, 2023, to February 26, 2024, to provide reasonable assurance that QuesTek Innovations' 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*.

Service Organization's Responsibilities

QuesTek Innovations 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 QuesTek Innovations' service commitments and system requirements were achieved. QuesTek Innovations has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, QuesTek Innovations 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 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.

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

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 QuesTek Innovations' service commitments and system requirements based on the applicable trust service criteria.

- Performing procedures to obtain evidence about whether controls within the system were effective to achieve QuesTek Innovations' 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 QuesTek Innovations' Platform were effective throughout the period November 27, 2023, to February 26, 2024, to provide reasonable assurance that QuesTek Innovations' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Insight Assurance LLC

Tampa, Florida
July 18, 2024

QUESTEK INNOVATIONS LLC'S MANAGEMENT ASSERTION

QUESTEK INNOVATIONS LLC

QUESTEK INNOVATIONS LLC' MANAGEMENT ASSERTION

We are responsible for designing, implementing, operating, and maintaining effective controls within QuesTek Innovations LLC's ('QuesTek Innovations) ICMD® Services System throughout the period November 27, 2023, to February 26, 2024, to provide reasonable assurance that QuesTek Innovations' 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 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 November 27, 2023, to February 26, 2024, to provide reasonable assurance that QuesTek Innovations' service commitments and system requirements were achieved based on the applicable trust services criteria. QuesTek Innovations' 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 November 27, 2023, to February 26, 2024, to provide reasonable assurance that QuesTek Innovations' service commitments and system requirements were achieved based on the applicable trust services criteria.

QuesTek Innovations LLC
July 18, 2024

ATTACHMENT A
DESCRIPTION OF THE BOUNDARIES OF THE ICMD® SERVICES SYSTEM

ATTACHMENT A

QUESTEK INNOVATIONS LLC'S DESCRIPTION OF THE BOUNDARIES OF ITS ICMD® SERVICES SYSTEM

SERVICES PROVIDED

ICMD® is a digital materials design platform including toolkits for materials design, accelerated qualification and certification, informatics and analytics, and simulation. Toolkits utilize QuesTek's Materials by Design® technology to provide proven models, datasets, and workflows, including third-party software and databases to support design processes. Access the expertise, models, and materials data generated over our 25-year history as pioneers and leaders in integrated computational materials engineering.

INFRASTRUCTURE

QuesTek Innovations maintains a system inventory that includes AWS, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents the device name, device type, vendor function, OS, location, and notes.

The QuesTek Innovations application infrastructure is located at AWS data centers. SSO acts as a hosting subservice organization for the company. The subservice organization provides the physical security and environmental protection controls, as well as managed services for QuesTek Innovations' infrastructure.

SSO's network security uses hardware and software-based intrusion prevention, advanced content filtering, anti-malware, and anti-spam modules.

In addition to the firewall, QuesTek Innovations uses anti-virus and anti-spyware applications to protect systems from viruses.

QuesTek Innovations' Information Security Policy and security procedures ensure that all computer devices (including servers, desktops, printers, etc.) connected to the QuesTek Innovations network have proper virus protection software, current virus definition libraries, and the most recent operating system and security patches installed. The IT department verifies that all known and reasonable defenses are in place to reduce network vulnerabilities while keeping the network operating. In the event of a virus threat, the anti-virus system will attempt to delete or quarantine the infected file. If the virus cannot be deleted or quarantined, the infected machine will be disconnected from the network and cleaned manually.

Multiple controls are installed to monitor traffic that could contain malicious programs or code. External perimeter scans are performed annually by a third-party vendor to expose potential vulnerabilities to the production environment and corporate data. Email is scanned at the gateway and in the hosted email environment. Server operating systems utilize anti-virus and anti-spyware programs. All employee workstation computers have a minimum standard hardware and software configuration. Employees are not allowed to install any software on QuesTek Innovations-owned

computers. The IT staff maintains several replacement computers that can replace workstations in need of repair or maintenance, thereby disrupting the employee's workday as little as possible.

Primary Infrastructure		
Category	**Description**	**Examples**
AWS Elastic Compute Cloud (EC2)	AWS	Compute system in the cloud
AWS Elastic Load Balancers	AWS	Load balance internal and external traffic
Virtual Private Cloud	AWS	Protects the network perimeter and restricts inbound and outbound access
S3 Buckets	AWS	Storage, upload, and download
AWS CloudFront	AWS	Masks S3 bucket paths
AWS CloudWatch	AWS	Monitoring service and log storage
AWS Internet Gateway	AWS	Allows communication between instances in your Amazon VPC and the Internet
AWS WAF	AWS	Web application firewall
Amazon RDS	AWS	Simplifies database management in the cloud

SOFTWARE

QuesTek Innovations maintains a list of critical software in use within its environment. The organization also retains appropriate software license documentation. Critical software in use includes the following:

Primary Software		
System/Application	**Operating System**	**Purpose**
AWS	Linux/ Windows	The cloud provider that hosts the ICMD® Software
Datadog	SaaS	Monitoring of cloud infrastructure
Sentry	SaaS	Error tracking and performance monitoring
GitHub	SaaS	Store, track, collaborate on software projects, and version control
Atlassian	SaaS	Collaborative tool for centralized knowledge repository

PEOPLE

The QuesTek Innovations staff provides support for the above services. QuesTek Innovations employs dedicated team members to handle all major product functions, including operations, and support. The IT Team monitors the environment, as well as manages data backups and

recovery. The Company focuses on hiring the right people for the right job as well as training them both in their specific tasks and on the ways to keep QuesTek Innovations and its data secure.

Chief Executive Officer (CEO) – Handles the strategic direction of the organization. The CEO assigns authority and responsibility to key management personnel with the skills and experience necessary to carry out their assignments.

Chief Commercial Officer (CCO) – Plans and directs all aspects of an organization's marketing and sales policies, objectives, and initiatives. Directs the planning, forecasting, marketing program development, partner relationship development, collateral material development, and customer satisfaction initiatives. Establishes short- and long-term sales goals and quotas in line with corporate objectives. Identifies key marketing outlets and competitive strategies that will enable the achievement of maximum sales volume. Manages a business unit, division, or corporate function with major organizational impact. Establishes overall direction and strategic initiatives for the given major function or line of business. Has acquired the business acumen and leadership experience to become a top function or division head.

Sales and Marketing – Directs the execution of the business development vision, strategy, plans, and processes to drive sales, increase revenue, expand markets, and accomplish financial objectives. Identifies and evaluates new markets, partners, channels, and customers. Develops and uses contacts and relationships within the industry, business environment, and customer base to understand and respond to competition, pricing, and product demand changes. Oversees the development of proposals and contracts for new business opportunities and manages negotiations. Collaborates with marketing, sales, product development, and other stakeholders to support business development plans. Manages a departmental sub-function within a broader departmental function. Creates functional strategies and specific objectives for the sub-function and develops budgets/policies/procedures to support the functional infrastructure.

Sales - Primary role for outbound reach to prospects and completing sales. They are also responsible for the maintenance and renewal of existing customer contracts.

Chief Information Officer – Responsible for the long-range direction of an organization's technology function. Directs the strategic design, acquisition, management, and implementation of an enterprise-wide technology infrastructure. Monitors and analyzes technology and trends that could improve the company's products and performance. Establishes technology standards and communicates technical information to the organization. Manages a business unit, division, or corporate function with major organizational impact. Establishes overall direction and strategic initiatives for the given major function or line of business. Has acquired the business acumen and leadership experience to become a top function or division head.

Technology and Engineering – This role is responsible for the operations of the day-to-day items to maintain the integrity of the environment. This role is also responsible for the provisioning of research and development of new and upcoming services within the company.

Operations and Support – This role includes the support team and crosses over to the engineering team. It is primarily responsible for daily support aspects of the business. This includes but is not limited to the support of end-users with day-to-day issues, as well as assisting in the onboarding, implementation, and migrations of new and existing customers as part of their ongoing maintenance.

DATA

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements. Customer data is captured which is utilized by QuesTek Innovations in delivering its ICMD® Services.

Information takes many forms. It may be stored on computers, transmitted across networks, printed, or written on paper, and spoken in conversations. All employees and contractors of QuesTek Innovations are obligated to respect and, in all cases, to protect confidential and private data. Customer information, employment-related records, and other intellectual property-related records are subject to limited exceptions, confidential as a matter of law. Many other categories of records, including company and other personnel records, and records relating to QuesTek Innovations' business and finances are, as a matter of QuesTek Innovations policy, treated as confidential. Responsibility for guaranteeing appropriate security for data, systems, and networks is shared by the Client Services and IT Departments. IT is responsible for designing, implementing, and maintaining security protection and retains responsibility for ensuring compliance with the policy. In addition to management and the technology staff, individual users are responsible for the equipment and resources under his or her control.

QuesTek Innovations has policies and procedures in place to ensure prior retention and disposal of confidential and private data. The retention and data destruction policies define the retention periods and proper destruction procedures for the disposal of data. These policies are reviewed at least annually. The destruction of data is a multi-step process. Client data is deleted upon termination of the contract. A ticket is created and assigned to the product team and system engineering team to coordinate the deletion of the data. First, all files received or generated from the client are identified and deleted by the system engineering team then the product team deletes all user-related data.

Electronic communications are treated with the same level of confidentiality and security as physical documents. Networks are protected by enterprise-class firewalls and appropriate enterprise-class virus protection is in place. Password protection with assigned user rights is required for access to the network, application, and databases. Access to the network, application, and databases is restricted to authorized internal and external users of the system to prohibit unauthorized access to confidential data. Additionally, access to data is restricted to authorized applications to prevent unauthorized access outside the boundaries of the system.

Data		
Category	**Description**	**Examples**
Public	Public information is not confidential and can be made public without any implications for QuesTek Innovations.	• Press releases • Public website
Internal	Access to internal information is approved by management and is protected from external access.	• Internal memos • Design documents • Product specifications • Correspondences
Customer data	Information received from customers for processing or storage by QuesTek Innovations. QuesTek Innovations must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Customer operating data • Customer PII • Customers' customers' PII • Anything subject to a confidentiality agreement with a customer
Company data	Information collected and used by QuesTek Innovations to operate the business. QuesTek Innovations must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Legal documents • Contractual agreements • Employee PII • Employee salaries • Research and Engineering Data

PROCEDURES

Formal IT policies and procedures exist that describe logical access, computer operations, change management, incident management, and data communication standards in order to obtain the stated objectives for network and data security, data privacy, and integrity for both the company and its clients and define how services should be delivered. These are communicated to employees and are located within the organization’s intranet.

ATTACHMENT B
PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

ATTACHMENT B

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

QuesTek Innovations designs its processes and procedures related to the QuesTek Innovations' ICMD® Services system ("System") to meet its objectives. Those objectives are based on the service commitments that QuesTek Innovations makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that QuesTek Innovations has established for the services.

QuesTek Innovations' commitments to users are communicated through Service Level Agreements (SLAs) or Master Service Agreements (MSAs), online Privacy Policy, and other customer agreements, as well as in the description of the service offering provided online.

Security Commitments

Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of services that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit.
- Use of data retention and data disposal.
- Uptime availability of production systems.

QuesTek Innovations establishes operational requirements that support the achievement of security, availability, and confidentiality, relevant laws and regulations, and other system requirements. Such requirements are communicated in system policies and procedures, system design documentation, and agreements with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition, how to carry out specific manual and automated processes required in the operation and development of the System.