The MathWorks, Inc.

SYSTEM AND ORGANIZATION CONTROLS (SOC 3) REPORT

MATHWORKS CLOUD-BASED APPLICATIONS SYSTEM

MATLAB® Online™, MATLAB Drive™, MATLAB® Grader™– LTI® Service, Online Training Courses, Online Licensing, MATLAB® Mobile™, Cloud Center, and ThingSpeak™

Edelstein & Company LLP
160 Federal Street, 9th Floor, Boston, MA 02110
www.edelsteincpa.com 617-227-6161

25 Braintree Hill Office Pk Suite 407, Braintree, MA 02184
www.ocd-tech.com 844-623-8324

TABLE OF CONTENTS

SECTION 1: ASSERTION OF THE MATHWORKS, INC. MANAGEMENT

Assertion of The MathWorks, Inc. Management

We, as the management of The MathWorks, Inc. ("MathWorks"), are responsible for designing, implementing, operating, and maintaining effective controls within MathWorks Cloud-Based Applications System (System) throughout the period February 1, 2023 through November 30, 2023, to provide reasonable assurance that MathWorks service commitments and system requirements relevant to security 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, as management of MathWorks are responsible for:

- Identifying the MathWorks Cloud-Based Applications System (System) and describing the boundaries of the System, which are presented in Attachment A

- Identifying our service commitments and system requirements

- Identifying the risks that would threaten the achievement of its service commitments and system requirements that are the objectives of our System, which are presented in Attachment B

- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the service commitments and system requirements

- Selecting the trust services categories that are the basis of our assertion

We have performed an evaluation of the effectiveness of the controls within the System throughout the period February 1, 2023 through November 30, 2023, to provide reasonable assurance that MathWorks service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022)* (AICPA, *Trust Services Criteria*).

In designing the controls over the System, we determined that certain trust services criteria can be met only if complementary user entity and subservice controls are suitably designed and operating effectively for the period February 1, 2023 through November 30, 2023.

MathWorks objectives for the System in applying the applicable trust services criteria are embodied in the service commitments and system requirements relevant to the applicable trust service criteria. The principal service commitments and system requirements related to the applicable trust service criteria are presented below, 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 must 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 February 1, 2023 through November 30, 2023, to provide reasonable assurance that MathWorks service commitments and system requirements were achieved based on the applicable trust services criteria.

The Management of The MathWorks, Inc.

SECTION 2: INDEPENDENT SERVICE AUDITORS' REPORT

Independent Service Auditors' Report

To: The Management of The MathWorks, Inc.

Scope:

We have examined MathWorks accompanying assertion titled Assertion of the Management of The MathWorks, Inc. (Assertion) that the controls within MathWorks Cloud-Based Applications System (System) were effective throughout the period February 1, 2023 to November 30, 2023, to provide reasonable assurance that MathWorks principal service commitments and System requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022) (AICPA, Trust Services Criteria).*

MathWorks utilizes Amazon Web Services (AWS) (subservice organization) to cloud-hosting services.

The description of the boundaries of the System (description) indicates that complimentary subservice organization controls that are suitably designed and operating effectively are necessary, along with the controls at MathWorks, to achieve the service organization's service commitments and the system requirements based on the applicable trust service criteria. The description presents the boundaries of the MathWorks system. Our examination did not extend to the services provided by AWS, and we have not evaluated the suitability of the design or operating effectiveness of such complimentary subservice organization controls.

The description indicates that complimentary user entity controls that are suitably designed and operating effectively are necessary, along with the controls at MathWorks, to achieve the service organization's service commitments and the system requirements based on the applicable trust service criteria. Our examination did not such complimentary user entity controls, and we have not evaluated the suitability of such controls.

Service Organization's Responsibilities

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

Service Auditors' 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 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.

An 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 MathWorks service commitments and system requirements based on the applicable trust services criteria; and

- Performing procedures to obtain evidence about whether controls stated within the System were effective to achieve MathWorks service commitments and system requirements based on the applicable trust services criteria.

4

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

Our examination was not conducted for the purpose of evaluating MathWorks cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

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

Inherent Limitations

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the 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, MathWorks management's assertion that the controls within MathWorks Cloud-Based Applications System were effective throughout the period February 1, 2023 to November 30, 2023, to provide reasonable assurance that MathWorks service commitments and system requirements were achieved based on the applicable trust services criteria, and if the subservice organization and user entity applied complimentary controls assumed in the design of MathWorks controls throughout the period, is fairly stated, in all material respects.

Edelstein & Company LLP

Boston, Massachusetts
April 16, 2024

ATTACHMENT A: MATHWORKS CLOUD-BASED APPLICATIONS SYSTEM

Company Overview and Background

Company Background

MathWorks (www.MathWorks.com) is a leading developer of software for technical computing and Model-Based Design. MathWorks develops, markets, and licenses its products to companies and users in over 100 countries on all seven continents. Its customers include 4,000,000 of the world's leading technical people, who work at the world's most innovative technology companies, research labs, financial institutions, and at more than 6,500 universities. MathWorks core products are MATLAB and Simulink. MATLAB is a programming environment for algorithm development, data analysis, visualization, and numeric computation. Simulink is a block diagram environment for simulation and Model-Based Design of multi-domain and embedded engineering systems. The company produces over 100 additional products for specialized tasks. MathWorks products are used throughout the automotive, aerospace, communications, electronics, and industrial automation industries as fundamental tools for research and development.

Overview of Products and Services

This section provides an overview of the products and services that are in scope of this system description.

MATLAB® Online™

MATLAB is a high-performance technical computing environment, which combines comprehensive math and graphics functions with a powerful high-level language. MATLAB Online is the online, browser-based version of the MATLAB software that provides access to the latest version of MATLAB from standard web browsers. Integration with MATLAB Drive enables users to store, access, and manage files with MATLAB Online.

MATLAB Online includes a feature called Simulink® Online™ which provides access to Simulink®, a simulation and model-based design environment that enables users to model and simulate systems and automatically generate code.

MATLAB® Drive™

MATLAB Drive provides a common cloud-based storage location for MATLAB files that integrates with MATLAB Online. Users can sync MATLAB Drive files to their local computer by installing MATLAB Drive Connector, a separate desktop program.

MATLAB® Grader™ - LTI® Service

MATLAB Grader allows instructors to create and share MATLAB-based interactive course assignments for their students, including rich text, images, hyperlinks, and LaTeX equations in problem descriptions and a library of reusable example problems, by using a browser-based authoring environment. MATLAB Grader – LTI® Service is a feature in MATLAB Grader that provides automatic grading of students' MATLAB code, real-time feedback to students, access to the latest version of MATLAB and toolboxes for use in assessments, and integration within a learning environment and gradebook using Learning Tool Interoperability (LTI) standards. (Learning Tools Interoperability (LTI)® is an education technology standard developed by the IMS Global Learning Consortium.)

Cloud Center

Cloud Center is a MathWorks hosted web application that enables customers to create, manage and access MATLAB and other MathWorks products on public cloud providers, such as AWS and Azure. Resources managed by Cloud Center are hosted in the customer's cloud account using credentials provided by the customer and linked to their Cloud Center account.
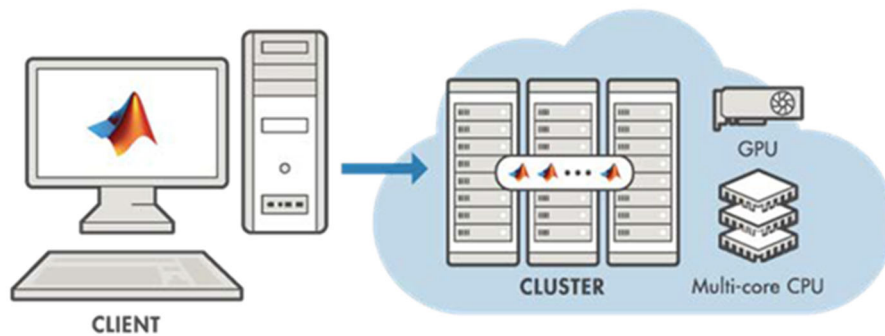
Online Training Courses

Online Training Courses provides free and paid online training courses about MathWorks products and their use in various applications. The course content is created by experts at MathWorks and is updated regularly to include the latest product features.

Courses can be accessed on-demand and consist of videos, reading materials, quizzes, and hands-on practice problems in which users interact with MATLAB in the context of the learning environment and receive automated feedback on their submissions. Most of the courses are accessible from a standard web browser while others can be accessed from MATLAB installed on laptop or desktop computers. A completion certificate is provided upon the completion of a course.

ThingSpeak

ThingSpeak™ is an IoT analytics service that allows users to aggregate, visualize, and analyze live data streams in the cloud. ThingSpeak provides instant visualizations of data posted by users' devices to ThingSpeak. With the ability to execute MATLAB® code in ThingSpeak, users can perform online analysis and process data as it comes in.

With ThingSpeak, users can store and analyze data in the cloud without configuring web servers, and sophisticated event-based email alerts can be triggered based on data coming in from the connected devices.

DATA AGGREGATION AND ANALYTICS

SMART CONNECTED DEVICES

ALGORITHM DEVELOPMENT SENSOR ANALYTICS
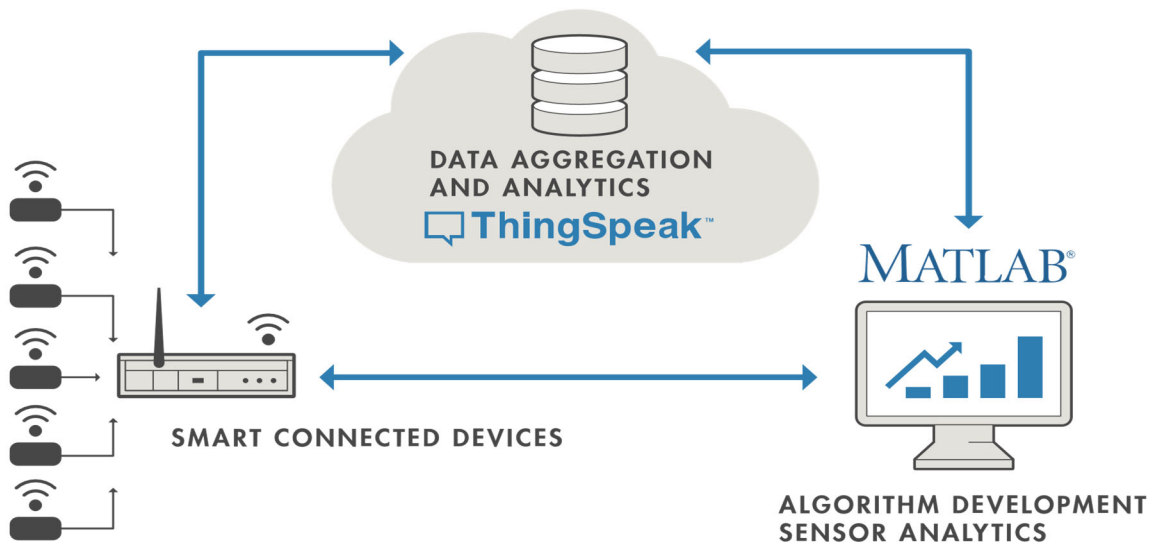
MATLAB® Mobile™

MATLAB® Mobile™ is a cloud service that allows users to connect their iOS and Android devices to the MathWorks Cloud. Using this service, users can store their files on MATLAB Drive and access them from any device running MATLAB Mobile™. Installing MATLAB Drive Connector allows users to synchronize files between their computers and MATLAB Mobile without the need to manually upload or download them. In addition to this, users can stream sensor data directly to the MathWorks Cloud for analysis in MATLAB Mobile or MATLAB Online or save the data to log files when they are offline.

Online Licensing

Online Licensing provides the ability to provision MathWorks software licenses from a cloud-based license manager. This provides license portability and is intended for customers who do not wish to host their own license server. This service supports various forms of licensing, such as on-demand, for selected MathWorks products. All systems in scope depend on the Online Licensing service.

Components of the System

Software

The applications in the system mentioned above are hosted on AWS cloud via a web server architecture. Application requests are routed to the web servers through Amazon AWS Route 53 DNS web service and Amazon AWS Load Balancers. User access is granted after successful authentication of a MathWorks account and verification of license for the user. Students and instructors access MATLAB Grader through their organization's Learning Management System. Outbound requests are routed back to the user through Amazon AWS CloudFront. Depending on the product, data is stored in Amazon RDS Database or Amazon DynamoDB.

Several applications are used to monitor system health and events across all services, such as:

Amazon GuardDuty	Monitors AWS accounts and workloads for malicious activity and unauthorized behavior
AWS CloudTrail	Supports governance, compliance, operational auditing, risk auditing and detecting unusual activity in AWS accounts

The company also uses other enterprise tools to monitor cloud security compliance, real-time event data, and its IT infrastructure.

Additional supporting software utilities to support the following activities are used by MathWorks to execute controls relevant to the in-scope applications but are not directly covered in this report:

- Work management for iterative software development
- Content collaboration and document management
- Source code management and version control
- Customer relationship management

The Systems in scope are dependent on the following internal applications/services although they are not directly covered in this report:

Data store	Cloud-based file system hosted on AWS that constitutes the underlying storage technology behind MATLAB Drive
Infrastructure services	MathWorks proprietary compute technology that supports MATLAB Online, MATLAB Grader, and Online Training Courses
MathWorks Account Management	Centralized framework for cloud-based authentication of MathWorks accounts for external customers across in-scope applications

Infrastructure

Each application in the System uses one or more of the following infrastructure components. MathWorks uses Amazon Web Services (AWS) as its subservice organization for infrastructure as a service (IaaS) hosting of the System in scope. The descriptions of the services below are provided by Amazon.

Amazon AWS Route 53	Highly available and scalable cloud Domain Name System (DNS) web service which connects user requests to infrastructure running in AWS
Amazon Simple Storage Service (Amazon S3)	Object storage service that helps organize data and configure finely tuned access controls to meet specific business, organizational, and compliance requirements
Amazon Elastic Compute Cloud (EC2)	Web service that provides secure, resizable compute capacity in the cloud

Amazon AWS Elastic Load Balancer	For automatic distribution of incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions
Amazon AWS CloudFormation	Provides a common language to model and provision AWS and third-party application resources in the cloud environment
Amazon AWS CloudFront	Content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds
Amazon RDS	Relational Database Service that supports key product functionality
Amazon DynamoDB	Key-value and document database that delivers single-digit millisecond performance at any scale
Amazon Simple Email Service	Cloud-based email sending service

Additional services are used by MathWorks to support its storage and application infrastructure, email services, and product development.

People

The personnel supporting the System include, but are not limited to the following:

- **Senior Management**: Includes the President and CEO of the company and all Vice-Presidents. They are responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives for the company.
- **Development**: Responsible for developing, testing, and releasing applications into production. This includes creating and maintaining product documentation, managing internal tools, providing quality assurance services, supporting internal process improvement, and training needs.
- **Legal Services**: Responsible for formulating policies that protect MathWorks intellectual property and support legal compliance.
- **Production Platform and Database Operations Teams**: Responsible for day-to-day management of the System ensuring application availability and security for internal users and customers.
- **System Services:** Responsible for providing enterprise infrastructure, IT process and tools and collaboration services.
- **MathWorks Security**: Responsible for information and product security.
- **Human Resources:** Responsible for hiring, performance management and communicating company-wide policies.
- **IT Training:** Responsible for creating and delivering IT training material and facilitating organizational/process change management.
- **Physical Security:** Responsible for protecting company assets, including, but not limited to, staff, facilities, equipment, and intellectual property through the implementation and management of a wide variety of safety and security policies, procedures, and programs.

Procedures

Standard operating procedures are documented for policies that need to be enforced at the company-level, department-level, or team-level. Along with these procedures, management has identified and put in place standards that ensure the achievement of objectives in the procedures. Control activities are established to guide the implementation of procedures.

MathWorks has developed and communicated policies relating to the following areas to its internal users:

- Change Management
- Risk Management
- Human Resources
- Internal Quality Assurance
- Physical Access Management
- Logical Access Management
- Asset Management
- Incident Management
- Vendor Relationship
- Encryption

Policies relevant to external customers are also published on the www.mathworks.com site:

- Privacy Policy
- Vulnerability Disclosure Policy

In addition to the above procedures, manual and automated control activities are described in the sections "Control Environment" and "Control Activities and Relevant Aspects of Operations" below.

Data

User Login Data Collection and Management

The system requires users to sign in with their MathWorks account, except for MATLAB Grader and certain courses in Online Training Courses. Users are encouraged to use a strong password to protect against unauthorized access. Users can choose to enable two-step verification for their MathWorks account to help safeguard against unauthorized access.

Where MATLAB Grader is accessed in conjunction with an educational institution's learning management system, MathWorks receives only anonymized user IDs through MATLAB Grader that MathWorks cannot associate to any individual. When MATLAB Grader is used in this manner, MathWorks does not store, process, or transmit personally identifiable information or confidential data in connection with MATLAB Grader. If customers have chosen to integrate the company's services with a third-party service, MathWorks may store authentication information received from the third-party service, in addition to information that MathWorks normally collects for its web site and online products and services.

For students and personnel at educational institutions that elect to use a federated identity management system, such as Shibboleth, the institution directs the user to a portal where the user signs in. After sign-in, MathWorks receives information from the institution including the user's identifier and organizational affiliation. If provided by the institution, MathWorks also receives the user's name and email address. The user then sets up his or her own MathWorks account, which is pre-populated with this information.

ThingSpeak requires users to sign in with their MathWorks Account. MathWorks stores any information that users provide for integration between ThingSpeak and MathWorks or third-party services, such as authentication credentials and code files. MathWorks also stores data that users choose to send to ThingSpeak. Users can choose to make that data public or private. Public data is generally displayed with the user's MathWorks Account login and a link to their MathWorks Account profile. Access to user private data and apps is protected by API keys that users may reset at any time.

Customer Data Collection and Management

The user's name, email address, country, and the reason for use of MathWorks products and services are required to create a MathWorks account. This information is provided by either the user or the user's organization at the time the account is created. When users are signed in with their MathWorks account, MathWorks can link their login and usage with licenses and subscriptions to MathWorks products and services to which the users have access.

For two-step verification, users provide an email address or phone number that is used for the purpose of sending verification messages.

The system contains technology that may send user experience information to MathWorks both in the course of normal usage and in the event of a software crash. This technology causes the system to send messages to MathWorks over the Internet that may contain network, device, license, and usage information. User experience information transmitted may include the products, features, and services accessed, length of session, errors that occurred, IP address, a license identifier, and the user's email address. MathWorks has technical and organizational restrictions in place that limit access to user experience information.

When users store files using the system, they are stored in MathWorks AWS cloud environment. If users are working offline, the files are stored on their own device until they are back online. Files stored online can only be accessed by the user who stored them unless the user chooses to share the files with others inside or outside the user's organization. Select MathWorks personnel serving in certain information technology roles have access to files stored online for purposes limited to deployment, backup, and recovery operations. These personnel have signed confidentiality agreements.

External user security commitments and how customer data is handled is published in customer privacy statement and online service agreement.

Subservice Organization Controls

MathWorks utilizes Amazon Web Services (subservice organization) to provide cloud-hosting services, including physical security and environmental safeguards, to support the MathWorks environment. According to its written documentation, it is expected that the subservice organization has implemented the following controls to support achievement of the associated criteria:

Criteria Reference	Expected Subservice Organization Controls
CC6.1, CC6.8	AWS applies a systematic approach to managing change to ensure changes to customer-impacting aspects of a service are reviewed, tested, and approved.
CC6.1	AWS enables customers to articulate who has access to AWS services and resources (if resource-level permissions are applicable to the service) that they own. AWS prevents customers from accessing AWS resources that are not assigned to them via access permissions. Content is only returned to individuals authorized to access the specified AWS service or resource (if resource-level permissions are applicable to the service).
CC4.1	AWS has a program in place for evaluating vendor performance and compliance with contractual obligations.
CC3.1, CC4.1	AWS has established a formal audit program that includes continual, independent internal and external assessments to validate the implementation and operating effectiveness of the AWS control environment.
CC6.8	AWS host configuration settings are monitored to validate compliance with AWS security standards and automatically pushed to the host fleet.
CC6.1, CC7.2, CC9.1	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment.
CC7.1	AWS performs application security reviews for externally launched products, services, and significant feature additions prior to launch to evaluate whether security risks are identified and mitigated.
CC7.1	AWS performs deployment validations and change reviews to detect unauthorized changes to its environment and tracks identified issues to resolution.
CC6.8, CC3.2, CC4.1, CC7.1, CC7.2	AWS performs external vulnerability assessments at least quarterly, identified issues are investigated and tracked to resolution in a timely manner.
CC6.1	EC2-Specific – AWS prevents customers from accessing custom AMIs not assigned to them by a property of the AMI called launch-permissions. By default, the launch-permissions of an AMI restrict its use to the customer/account that created and registered it.
CC6.1	EC2-Specific – AWS prevents customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software.
CC6.1, CC6.6	EC2-Specific – Physical hosts have host-based firewalls to prevent unauthorized access.

CC6.1	EC2-Specific – Virtual hosts are behind software firewalls which are configured to prevent TCP/IP spoofing, packet sniffing, and restrict incoming connections to customer-specified ports.
CC7.2	Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
CC6.1, CC6.6, CC7.1	Firewall devices are configured to restrict access to the computing environment and enforce boundaries of computing clusters.
CC6.1, CC6.2, CC6.8	IT access privileges are reviewed on a quarterly basis by appropriate personnel.
CC6.1	KMS-Specific – AWS Services that integrate with AWS KMS for key management use a 256-bit data key locally to protect customer content.
CC6.1	KMS-Specific – Customer master keys created by KMS are rotated on a defined frequency if enabled by the customer.
CC6.1	KMS-Specific – Customer master keys used for cryptographic operations in KMS are logically secured so that no single AWS employee can gain access to the key material.
CC6.1	KMS-Specific – KMS endpoints can only be accessed by customers using TLS with cipher suites that support forward secrecy.
CC6.1, CC6.4	KMS-Specific – Recovery key materials used for disaster recovery processes by KMS are physically secured offline so that no single AWS employee can gain access to the key material.
CC6.1	KMS-Specific – Requests in KMS are logged in AWS CloudTrail.
CC6.1	KMS-Specific – The key provided by KMS to integrated services is a 256-bit key and is encrypted with a 256-bit AES master key unique to the customer's AWS account.
CC6.1, CC6.6, CC6.8, CC7.2	Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
CC6.4	Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
CC6.4	Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
CC6.4	Physical access to server locations is reviewed on a quarterly basis by appropriate personnel.
CC6.1, CC6.6	S3-Specific – External data access is logged with the following information: data accessor IP address, object, and operation. Logs are retained for at least 90 days.
CC6.1	S3-Specific – S3 generates and stores a one-way salted HMAC of the customer encryption key. This salted HMAC value is not logged.

CC6.1	VPC-Specific – Network communications within a VPC are isolated from network communications within other VPCs.
CC6.1	VPC-Specific – Network communications within a VPN Gateway are isolated from network communications within other VPN Gateways.

Complementary Controls at User Entities

Controls and policies at the MathWorks have been created with the assumption that its customers (user entities) have controls in place within their organizations. The following is a representative list of controls that are recommended to be in operation at user entities to complement the controls of MathWorks system. This is not a comprehensive list of all controls that should be employed by MathWorks user entities.

Criteria Reference	Complementary User Entity Control (CUEC)
CC6.1, CC6.3, CC6.6, CC6.7, CC6.8, CC7.1	User entities secure the software and hardware used to access MathWorks products.
CC6.1, CC6.2, CC6.3, CC6.6	User entities establish, execute and monitor controls pertaining to the use of system IDs and passwords, and access to the user entity's resources (including MathWorks products).
CC6.1	User entities are responsible for managing their users' password authentication mechanism.
CC3.2, CC7.2, CC7.3, CC7.4, CC7.5, CC9.2	User entities are responsible for reviewing security bug reports published by MathWorks.
CC6.1, CC6.6	User entities are responsible for configuring application parameters in a secure manner by reviewing MathWorks documentation, where applicable.
CC7.2, CC9.2	User entities are responsible for training end-users.
CC2.2, CC2.3, CC7.3	User entities are responsible for reporting any identified security issues to the MathWorks.
CC6.1, CC6.7	User entities enforce desired level of encryption for network sessions.
CC6.3	User entities are responsible for the sharing permissions of content in the in-scope applications, where applicable.
CC6.1, CC6.7	User entities enforce desired level of security on devices they choose to use for local synchronization of their MATLAB files.
CC2.3, CC6.5, CC6.7, CC7.5	User entities are responsible for understanding and adhering to the contents of their service contracts, including commitments related to system security.
CC2.1	User entities are responsible for managing their data inputs, and data uploads to in-scope applications for completeness, accuracy, and timeliness.

ATTACHMENT B: PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Principal Service Commitments and System Requirements

MathWorks designs its processes and procedures related to its System to meet its objectives for providing its Cloud-based Applications System. Those objectives are based on the service commitments that MathWorks makes to user entities.

Service Commitments made to user entities are documented and communicated in customer agreements, as well as, in the description of the service offering provided on the MathWorks website. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental design of the MathWorks Cloud-based Applications System are intended to permit MathWorks users to access the information and resources they need on the infrastructure supporting the System 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.

MathWorks Cloud-Based Applications System establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in MathWorks Cloud-based Applications System policies and procedures, system design documentation, and contracts 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 to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the MathWorks Cloud-Based Applications System.